DEFEND | DETECT | RESPOND | RESILIENT

RADAR

# MODERN CYBER WARFARE

&

# THREAT INTELLIGENCE HANDBOOK

A TECHNICAL ANALYSIS OF

## RUSSIA'S CYBER OPERATIONS AGAINST UKRAINE (2022–2023)

BASED ON CERT-UA ANALYTICAL REPORTS (2022–2023)

SOC ANALYSTS DFIR ANALYSTS THREAT INTEL ANALYSTS SECURITY ENGINEERS CERT TEAMS

*"Cyber warfare is no longer a supporting activity — it is an operational domain equal to **land, sea, air, space, and the electromagnetic spectrum.**"*

ROHIT DINDE

FIRST EDITION • 2026

FRONT MATTER

# Copyright & Disclaimer

## MODERN CYBER WARFARE & THREAT INTELLIGENCE HANDBOOK

*A Technical Analysis of Russia's Cyber Operations Against Ukraine (2022–2023)*



### DEFENSIVE USE STATEMENT

This handbook has been prepared exclusively for educational, research, professional development, and defensive cybersecurity purposes. It synthesizes publicly available threat intelligence, operational observations, and defensive methodologies to strengthen cyber resilience and improve organisational security posture.

**This publication is NOT intended to facilitate unauthorized access, offensive cyber operations, or malicious activity of any kind.**

### PRIMARY REFERENCES

This handbook is primarily based on publicly available analytical reports published by CERT-UA (Computer Emergency Response Team of Ukraine) during 2022–2023, together with established cybersecurity frameworks and defensive best practices, including MITRE ATT&CK, NIST CSF 2.0, NIST SP 800-61 Rev.2, CISA Shields Up guidance, ENISA Threat Landscape reports, and NATO CCDCOE research.

ISBN: To be assigned
VERSION: 1.0
PUBLICATION YEAR: 2026

rohitdinde30@gmail.com
github.com/Rohit30Confluence
linkedin.com/in/rohitdinde

FRONT MATTER

# Foreword

Modern warfare has evolved beyond the physical battlefield. In the twenty-first century, control of information, networks, and critical infrastructure is as decisive as control of territory.

The Russia–Ukraine conflict has demonstrated how cyber operations can influence strategic outcomes, shape military campaigns, and target the foundations of national resilience. What makes this conflict unique is the unprecedented volume of publicly documented cyber activity — thanks in large part to the transparency and professionalism of organisations such as CERT-UA.

This handbook transforms those operational observations into a structured, practitioner-focused resource. It is written for defenders — analysts, engineers, responders, and leaders — who must detect, respond to, and withstand today's cyber threats.

Its purpose is not to describe how attacks are performed, but how they can be understood, anticipated, and defeated.

May this handbook help build stronger defenders, more resilient systems, and a more secure digital world.

> "
>
> **INFORMATION IS THE OXYGEN OF THE MODERN BATTLEFIELD.**
>
> "

★ ★ ★

Rohit Dinde

Author — Pune, India — May 2026

**THIS HANDBOOK IS DEDICATED TO**

| THE ANALYSTS | THE RESPONDERS | THE ENGINEERS | THE LEADERS | THE DEFENDERS |
|---|---|---|---|---|
| Who detect the unseen | Who act under pressure | Who build defences | Who make critical decisions | Who stand for resilience |

FRONT MATTER

# Table of Contents



*(Continued in Part II — not included in this excerpt)*

PART

# I

# FOUNDATIONS OF MODERN CYBER WARFARE

## UNDERSTANDING CYBER CONFLICT IN THE TWENTY-FIRST CENTURY

🛡 EVOLUTION 🌐 CONFLICT 🎯 INTELLIGENCE 🔗 HYBRID WARFARE 🚦 LESSONS

> *"Future conflicts will be won not only by those who dominate the physical battlefield,*
> *but also by those who control information, networks, and digital infrastructure."*

CHAPTER 1

# INTRODUCTION TO MODERN CYBER WARFARE

> *“Cyber power is the ability to use cyberspace to create advantages and influence events across all domains.”*

This chapter introduces the conceptual foundations of modern cyber warfare, tracing its evolution from isolated incidents of the 1990s to a fully integrated operational domain within contemporary military strategy, using the Russia–Ukraine conflict as its central case study.

# Executive Summary

The CERT-UA analytical reports collectively demonstrate a significant transition in Russian cyber operations between 2022 and 2023. While the early stages of the conflict emphasized disruptive attacks, destructive malware, and denial-of-service operations, subsequent campaigns increasingly prioritized long-term intelligence collection, credential theft, persistence, and operational support for military objectives.

### 💡 STRATEGIC OBSERVATION

Modern cyber campaigns increasingly prioritize long-term intelligence value over immediate disruption — a shift with direct implications for how defenders allocate detection and monitoring resources.

### WHAT THIS CHAPTER COVERS

- Foundational concepts of cyber warfare as a military domain
- Historical evolution from the 1990s to present day
- Structural overview of the Russia–Ukraine cyber conflict
- The cyber kill chain and intelligence cycle frameworks

### WHO THIS CHAPTER IS FOR

- SOC analysts building situational awareness
- Threat intelligence teams tracking adversary trends
- CERT and incident response personnel
- Government and defense cybersecurity leadership

# Core Goals of Modern Cyber Warfare

**Intelligence Collection**
Acquire information supporting strategic decision-making.

**Infrastructure Disruption**
Reduce the availability, reliability, and integrity of critical services.

**Military Support**
Support military operations and battlefield objectives.

**Information Influence**
Shape perception, narratives, and public decision-making.

**Long-Term Persistence**
Maintain covert access for future operations and exploitation.

### INTELLIGENCE NOTE

CERT-UA reporting consistently shows that intelligence collection became the dominant objective throughout 2023, gradually surpassing disruptive intent as the primary driver of observed campaigns.

# Evolution of Cyber Warfare

| | |
|---|---|
| **1990s** | Early cyber experimentation by state and non-state actors. |
| **2007** | Estonia cyber attacks — the first large-scale cyber attacks on a nation-state's infrastructure. |
| **2008** | Georgia conflict — cyber operations observed alongside kinetic military actions. |
| **2014** | Ukraine conflict begins — destructive malware, ICS attacks, and cyber-espionage escalate. |
| **2022** | Full-scale invasion of Ukraine — cyber operations expand in scale, sophistication, and coordination. |
| **2023&beyond** | Persistent campaigns focused on espionage, credential theft, and long-term positioning. |

**KEY TAKEAWAY**

Each major conflict since 2007 has expanded the scope and integration of cyber operations within broader military and strategic planning, culminating in the deeply hybridized model observed in Ukraine since 2022.

# Russia–Ukraine Conflict Overview

### GEOPOLITICAL CONTEXT

The Russia–Ukraine conflict represents one of the first large-scale wars in which cyber operations are deeply integrated with conventional military campaigns, intelligence operations, and information warfare, generating an unprecedented volume of publicly documented incident data.

## Primary Operational Targets

**Government**
Disruption, espionage, and data theft.

**Energy Sector**
Induce outages and operational impact.

**Telecom**
Enable surveillance, disruption, control.

**Defence Industry**
Intel gathering on capabilities and R&D.

**Logistics**
Disrupt supply chains and mobility.

**Financial**
Undermine financial stability and trust.

# Cyber Campaign Timeline (2022–2023)

### 2022

**H1 — Early Conflict**
Disruptive attacks, wipers, DDoS, and network disruption.

**H2 — Shift to Espionage**
Increase in credential theft, lateral movement, and data exfiltration.

### 2023

**H1 — Persistence Phase**
Long-term access, living-off-the-land techniques, and data collection.

**H2 — Targeted Operations**
Focus on telecom, supply chain, automation, and cloud services.

**KEY TREND**

From disruption and destruction towards intelligence and persistence — a maturation pattern consistent with a long-duration, resource-constrained conflict.

# Hybrid Warfare in the Digital Age

Hybrid warfare blends multiple instruments of national power into a single, coordinated campaign. Cyber operations rarely occur in isolation — they are woven into a broader effort spanning military, economic, diplomatic, and informational domains.

### MILITARY OPERATIONS

Coordination with kinetic action and battlefield objectives.

### CYBER OPERATIONS

Intrusion, disruption, espionage, and access operations.

### DIPLOMATIC PRESSURE

Leverage cyber incidents in negotiation and signaling.

### INFORMATION WARFARE

Narrative shaping, disinformation, and influence operations.

### ECONOMIC PRESSURE

Targeting financial systems and economic stability.

### INTELLIGENCE OPERATIONS

Sustained collection supporting strategic planning.

### STRATEGIC OBSERVATION

Hybrid warfare blurs the boundaries between peace, crisis, and open conflict — requiring defenders to treat cyber resilience as a continuous, not episodic, discipline.

# Cyber Kill Chain

A widely-used, publicly documented conceptual model (Lockheed Martin) for describing the general stages of an intrusion — used here purely to structure defensive detection and response planning.

1. **Reconnaissance**
   Gather information about the target.
2. **Weaponization**
   Prepare the payload and delivery method.
3. **Delivery**
   Transmit the payload to the target.
4. **Exploitation**
   Trigger a vulnerability to gain access.
5. **Installation**
   Install malware or a backdoor for persistence.
6. **Command & Control**
   Establish a C2 channel with the compromised host.
7. **Actions on Objectives**
   Achieve the mission objective (data theft, disruption, etc.).

# Intelligence Cycle

### 1. Planning
Define requirements and objectives for the intelligence effort.

### 2. Collection
Gather data from multiple sources across the environment.

### 3. Processing
Validate, correlate, and organize raw data into usable form.

### 4. Analysis
Evaluate and produce actionable intelligence products.

### 5. Dissemination
Deliver findings to relevant decision makers.

### 6. Feedback
Assess and improve the process for future cycles.

This cycle repeats continuously: mature threat-intelligence programs treat it as a loop rather than a linear process, feeding lessons from each cycle back into planning.

# Key Lessons Learned

**OPERATIONAL LESSONS**

- Attacker objectives evolved rapidly across the conflict timeline.
- Espionage became the dominant long-term goal.
- Credential theft is a key enabler of persistence.
- Telecommunications remain high-value strategic targets.
- Use of legitimate/native tools reduces detectability.

**DEFENSIVE PRIORITIES**

- Continuous monitoring and visibility across environments.
- Strong identity & access management practices.
- Network segmentation and zero-trust architecture.
- Threat-informed detection engineering.
- Coordinated incident response and information sharing.

# Chapter Summary

**KEY TAKEAWAYS**

- Cyber operations are fully integrated into modern military strategy.
- Russian cyber campaigns shifted from disruption toward long-term espionage.
- Credential theft and persistence are central to attacker success.
- Critical infrastructure — especially telecom and energy — remain primary targets.
- Resilient defense depends on visibility, detection, and coordination.

The remainder of this handbook builds on these foundations, examining the threat-actor landscape, operational evolution across 2022–2023, and structured intelligence-assessment methodology in Part II.

# Further Reading

**CERT-UA Annual Reports (2022–2023)**
Official Ukrainian government analytical reporting.

**MITRE ATT&CK Enterprise Framework**
Public knowledge base of adversary tactics and techniques.

**NIST Cybersecurity Framework 2.0**
Guidelines for managing cybersecurity risk.

**NIST SP 800-61 Rev. 2**
Computer security incident handling guide.

**CISA Shields Up Guidance**
Cybersecurity awareness and hardening recommendations.

**ENISA Threat Landscape Reports**
European Union threat-landscape assessments.

**NATO CCDCOE Publications**
Cyber-defence and resilience research.

CHAPTER 2

# UNDERSTANDING THE ADVERSARY

Modern cyber defence begins by understanding who is conducting operations — not just how.

Russian cyber operations consist of multiple entities with different responsibilities and objectives. These organizations pursue strategic goals aligned with national priorities rather than financial gain.


### STRATEGIC OBSERVATION

Russian cyber operations are conducted through multiple organizations with overlapping responsibilities rather than a single centralized entity.

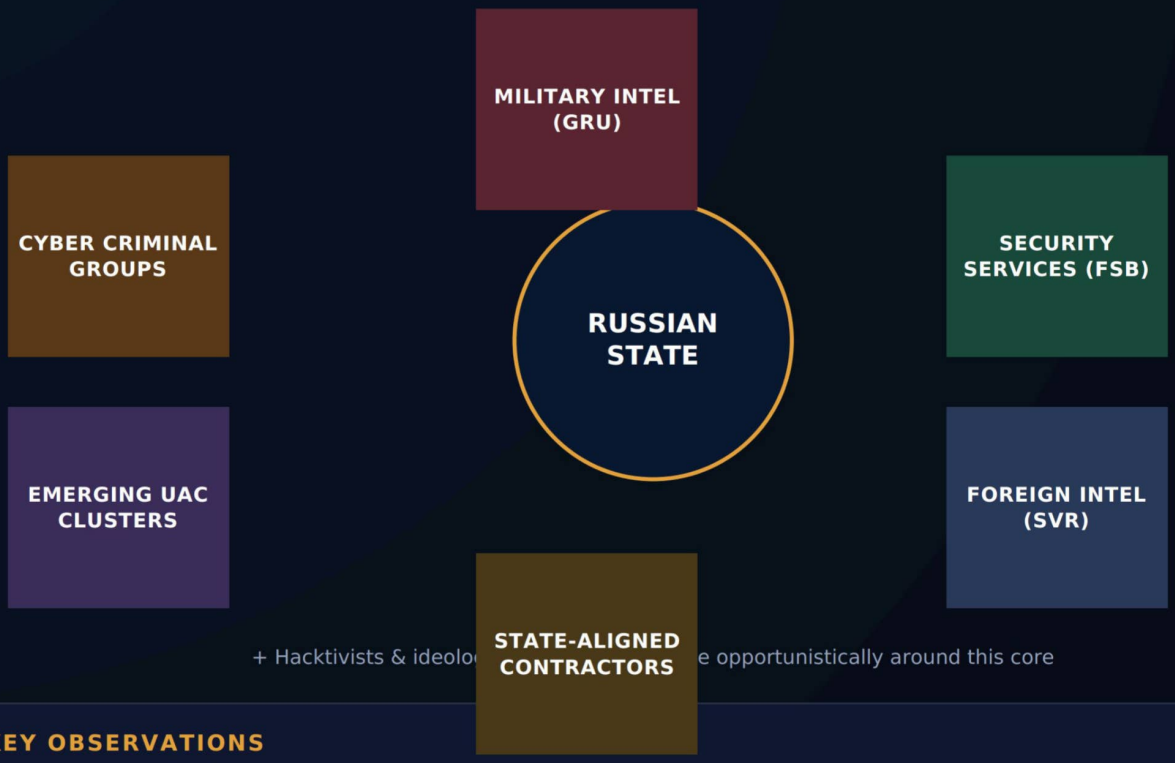
Unlike financially motivated attackers, these entities pursue strategic objectives aligned with national priorities.

### KEY TAKEAWAY

Understanding the structure and roles of these entities is essential for accurate threat assessment and effective defence.

# RUSSIAN CYBER ECOSYSTEM

The CERT-UA reports show that Russian cyber operations involve a diverse ecosystem of state and non-state actors working independently or in coordination.




+ Hacktivists & ideolo e opportunistically around this core

### KEY OBSERVATIONS

- Roles and activities often overlap and interact between different entities.
- Different entities collaborate or support overlapping objectives.
- Tactics, tools, and procedures evolve rapidly to evade detection and response.
- New actors emerge and adapt quickly to changing conditions.

# GAMAREDON (UAC-0010)

One of the most persistent threat groups documented by CERT-UA.

## THREAT ACTOR PROFILE

| | |
|---|---|
| Alias | **UAC-0010 (Gamaredon)** |
| First Observed | **2013** |
| Threat Level | **VERY HIGH** |
| Activity Status | **Highly Active** |
| Primary Mission | **Espionage & Intel Collection** |

## PRIMARY TARGETS

- Government entities
- Defence & military
- Border security services
- Law enforcement agencies

## OBJECTIVES

- Intelligence collection
- Credential theft
- Long-term persistence
- Military intel support

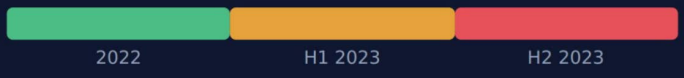
## TYPICAL TECHNIQUES

- Spear phishing
- Malicious documents
- Script-based malware (VBS/PowerShell)
- Use of legitimate tools

## PERSISTENCE METHODS

- Registry Run keys
- Scheduled tasks
- Web shells
- Encrypted C2 channels

## ACTIVITY TIMELINE




## ANALYST ASSESSMENT

Gamaredon remained highly active throughout the reporting periods, particularly in espionage-focused operations targeting Ukrainian government and defence entities.

# GAMAREDON ATTACK LIFECYCLE

Typical infection and operation chain observed in Gamaredon campaigns.

1. **Reconnaissance** Collect info via OSINT, public records, social engineering.
2. **Phishing Email** Send spear-phishing with malicious attachments or links.
3. **User Opens Attachment** Target opens the malicious file or enables macros.
4. **Initial Malware** Execution of script-based malware (VBS, PowerShell).
5. **Credential Collection** Harvest credentials, tokens, cookies, system data.
6. **Persistence** Establish persistence via multiple techniques and scheduled tasks.
7. **Command & Control** Establish encrypted communication with C2 infrastructure.
8. **Document Exfiltration** Collect and exfiltrate sensitive documents and intelligence.

## BLUE TEAM PRIORITY CONTROLS

- ✉ Email Security — Filtering & sandboxing
- Multi-Factor Auth — MFA everywhere
- Endpoint Detection — EDR coverage
- Script Monitoring — PowerShell & AMSI logging

## DETECTION OPPORTUNITIES (MAP TO MITRE ATT&CK)

| RECONNAISSANCE | INITIAL ACCESS | EXECUTION | PERSISTENCE | C2 COMMUNICATION |
|---|---|---|---|---|
| T1593 — Search Open Websites | T1566 — Phishing | T1059 — Command & Scripting | T1547 — Boot / Logon Autostart | T1071 — Application Layer Protocol |

# SANDWORM (UAC-0082)

Threat group associated with disruptive operations against critical infrastructure.

## THREAT ACTOR PROFILE

| | |
|---|---|
| Alias | **UAC-0082 (Sandworm)** |
| First Observed | **2009 (publicly attributed)** |
| Threat Level | CRITICAL |
| Primary Mission | **Infrastructure Disruption** |

## MAIN TARGETS

Energy | Telecom | ICS/SCADA | Government

## OPERATIONAL CHARACTERISTICS

- Advanced capabilities targeting operational technology (OT).
- Strong expertise in ICS/SCADA environments.
- Ability to cause physical and operational disruption.
- Often combines destructive wipers with espionage tools.

## OPERATIONAL OBJECTIVES

- Disrupt critical infrastructure operations.
- Conduct intelligence gathering.
- Degrade services and cause chaos.
- Maintain strategic long-term access.

## SELECTED HISTORICAL OPERATIONS (PUBLIC REPORTING)

| | |
|---|---|
| **2015** | Power grid attacks in Ukraine (publicly attributed to BlackEnergy / KillDisk). |
| **2016** | Telecommunication provider incidents. |
| **2017** | NotPetya-like global impact incidents. |
| **2022** | Destructive malware deployed during the invasion. |
| **2023** | Continued targeting of telecom and critical infrastructure. |

# SANDWORM OPERATIONAL MODEL

Typical attack flow targeting critical infrastructure and organizations.

1. **Internet Reconnaissance**
   Identify public-facing services and vulnerable entry points.
2. **Public Service / Perimeter**
   Exploit vulnerabilities in internet-facing services.
3. **Initial Access**
   Gain foothold using exploits or spearphishing.
4. **Internal Network Access**
   Move inside the network, establish initial presence.
5. **Privilege Escalation**
   Obtain higher privileges and compromise privileged accounts.
6. **Lateral Movement**
   Move across systems to expand access and control.
7. **Domain / Environment Control**
   Achieve domain admin or environment-wide control.
8. **Operational Impact**
   Disrupt, degrade, or steal data to achieve objectives.

## BLUE TEAM — DETECTION OPPORTUNITIES

- Monitor exposed services and vulnerabilities
- Detect unusual logins and lateral movement
- Alert on privilege escalation attempts
- Identify C2 traffic and anomalous communications
- Monitor changes to domain controllers and critical systems

# GRU OPERATIONS

Main Directorate of the General Staff of the Armed Forces of the Russian Federation. GRU cyber units conduct offensive operations in support of military objectives and strategic interests.

## PRIMARY OBJECTIVES

- Support military operations and battlefield intelligence.
- Gather intelligence on logistical networks and supply chains.
- Target energy, telecommunications, and critical infrastructure.
- Collect information for defence planning and military operations.

## TYPICAL TARGETS

- Defence organizations
- Military units
- Energy & utilities
- Telecommunications
- Government infrastructure
- Logistics & transport

## OBSERVED OPERATIONS

- Conducts both espionage and disruptive operations.
- Integrates cyber operations with kinetic and information operations.
- Targets critical infrastructure to enable military advantage.
- Uses a mix of custom tools and commodity malware.

## ANALYST ASSESSMENT

THREAT LEVEL: VERY HIGH

## STRATEGIC NOTE

GRU operations demonstrate close alignment with military campaigns and are increasingly synchronized with other domains of warfare.

# FSB OPERATIONS

Federal Security Service of the Russian Federation. The FSB conducts long-term intelligence collection operations with a strong emphasis on persistence and stealth.

## OPERATIONAL PRIORITIES

- Maintain long-term access.
- Steal sensitive documents and data.
- Harvest credentials and monitor emails.
- Compromise government and critical sector entities.
- Prepare access for future operations.

## TYPICAL TARGETS

- Government agencies
- State institutions
- Defence & security sectors
- Research organizations
- Critical infrastructure

## OPERATIONAL CHARACTERISTICS

- Highly persistent and patient operations.
- Focus on stealth rather than destruction.
- Extensive use of credential theft and email compromise.
- Utilizes custom backdoors and living-off-the-land techniques.

## ANALYST ASSESSMENT

THREAT LEVEL: HIGH

## STRATEGIC NOTE

FSB-linked groups prioritize intelligence value and long-term presence over immediate impact.

# SVR OPERATIONS

Foreign Intelligence Service of the Russian Federation. The SVR focuses on strategic intelligence collection to support Russian foreign policy and geopolitical objectives.

## OPERATIONAL PRIORITIES

- Collect diplomatic and political intelligence.
- Monitor international organizations.
- Obtain strategic, economic, and policy information.
- Support long-term geopolitical objectives.
- Maintain discreet and covert operations.

## TYPICAL TARGETS

- Diplomatic missions
- International organizations
- Government ministries
- Think tanks & research institutes
- Media & policy organizations

## OPERATIONAL CHARACTERISTICS

- Emphasis on stealth, discretion, and deniability.
- Long-term espionage and strategic intelligence gathering.
- Often uses subtle intrusion techniques and insider access.
- Less focused on disruptive operations.

## ANALYST ASSESSMENT

THREAT LEVEL: MEDIUM

## STRATEGIC NOTE

SVR operations are primarily intelligence-driven and aim to influence policy and strategic decision-making rather than cause operational disruption.

# EMERGING THREAT GROUPS (2023)

New and evolving actors observed prominently during H2 2023.

### REMCOS RAT

Remote access trojan used for persistence and system control.

**Impact: High**

### LUMMASTEALER

Information stealer targeting credentials and browser data.

**Impact: High**

### MEDUZASTEALER

Steals sensitive data, crypto wallets, and authentication data.

**Impact: High**

### REMOTE UTILITIES

Legitimate remote administration tools abused in attacks.

**Impact: Medium**

### FINANCIALLY MOTIVATED GROUPS

Operate ransomware, stealers, and fraud campaigns.

**Impact: High**

### RAPID ADAPTATION

Quickly adopt new tools, techniques, and evade detection.

**Impact: High**

### THREAT EVOLUTION TREND (2022–2023)

| EARLY 2022 | LATE 2022 | H1 2023 | H2 2023 | LATE 2023+ |
|---|---|---|---|---|
| Disruption Focused | Espionage Focused | Persistence Focused | Credential Theft / Telecom Focus | Financial Crime / Multi-Motive |

### KEY OBSERVATIONS

- New groups are well-resourced and technically capable.
- Increased use of information stealers and remote access tools.
- Financial motives are increasingly intertwined with espionage.
- Adaptation speed of adversaries continues to increase.

# COMPARATIVE THREAT ACTOR MATRIX

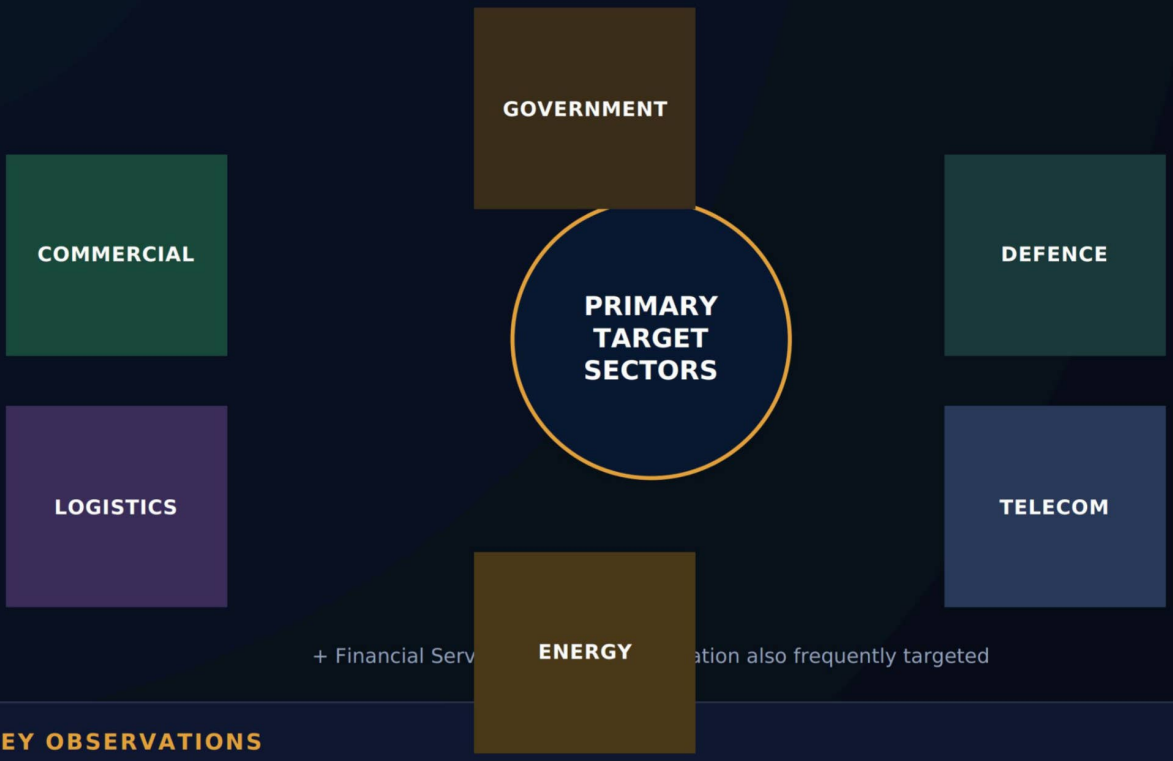
Observed patterns across major threat actors (2022–2023).

| THREAT ACTOR | PRIMARY GOAL | TYPICAL TARGETS | SOPHISTICATION | PERSISTENCE | IMPACT |
|---|---|---|---|---|---|
| **Gamaredon** (UAC-0010) | Espionage & Intel Collection | Government, Defence, Border Security | ★★★★☆ | Very High | High |
| **Sandworm** (UAC-0082) | Infrastructure Disruption | Energy, Telecom, ICS, Gov Infrastructure | ★★★★★ | High | Critical |
| **APT28** (UAC-0001) | Military Intelligence | Defence, Military, Government Agencies | ★★★★☆ | Very High | High |
| **FSB-linked Groups** | Long-term Access & Intel | Government, State Institutions | ★★★★☆ | Very High | High |
| **SVR-linked Groups** | Strategic Intelligence | Diplomatic Entities, Policy Institutions | ★★★★☆ | High | Medium |
| **Criminal Groups** | Financial Gain | Commercial Organizations, Individuals | ★★★☆☆ | Medium | Medium |
| **Emerging UAC Groups** | Mixed (Espionage/Financial/Access) | Government, Commercial, Telecom, Finance | ★★★☆☆ | High | High |

ℹ Attribution in cyber operations can be complex and may evolve as new evidence emerges. This matrix summarizes patterns observed in CERT-UA reports rather than providing definitive attribution for every campaign.

# SECTOR TARGETING

Recurring target sectors observed across 2022–2023.




+ Financial Serv ation also frequently targeted

### KEY OBSERVATIONS

- Telecommunications and energy sectors faced the highest volume of targeted operations in 2023.
- Government and defence entities remain prime intelligence objectives.
- Increasing overlap with commercial and financial sectors for data theft and financial gain.

# EVOLUTION OF OBJECTIVES

Shift in operational focus observed from 2022 through 2023.

**EARLY 2022**

### Disruption

Widespread destructive attacks targeting critical infrastructure and government systems — focus on causing immediate impact and chaos.

**LATE 2022**

### Espionage

Increased emphasis on intelligence collection, reconnaissance, and situational awareness to gather information supporting military operations.

**H1 2023**

### Persistence

Building long-term access, lateral movement, and establishing resilient footholds to maintain access for future operations.

**H2 2023**

### Telecom & Credential Theft

Targeting telecom providers, identity systems, and credential harvesting at scale to exploit identity for deeper access and fraud.

**H2 2023**

### Financial Crime

Rise in financially motivated campaigns converting access and data theft into monetization.

**STRATEGIC INSIGHT**

The trend shows a transition from short-term disruptive impact to long-term strategic advantage through intelligence, persistence, and financial exploitation.

# KEY DEFENSIVE LESSONS

Actionable priorities for strengthening cyber resilience.

### ACCESS SECURITY

- Enforce Multi-Factor Authentication (MFA)
- Implement Privileged Access Management (PAM)
- Apply least privilege principles

### ENDPOINT DEFENCE

- Deploy EDR/XDR solutions
- Keep systems and applications updated
- Enable application allowlisting

### NETWORK RESILIENCE

- Implement segmentation
- Monitor east-west traffic
- Use IDS/IPS and NDR solutions

### EMAIL & WEB SECURITY

- Advanced email filtering
- Sandboxing for attachments & links
- DNS & web content filtering

### THREAT DETECTION

- Continuous monitoring (SIEM, UEBA)
- Threat hunting programs
- Anomaly detection use-cases

### INCIDENT RESPONSE

- Maintain updated IR plans
- Conduct regular simulations
- Ensure rapid containment capabilities

### THREAT INTELLIGENCE

- Consume reliable threat intelligence
- Share indicators with trusted partners
- Enrich detections

### PEOPLE & PROCESS

- Security awareness training
- Clear escalation procedures
- Strong security culture

**CORE PRINCIPLE**

**Detect early. Respond fast. Recover strong. Share always.**

END OF PART II

# THREAT ACTORS & OPERATIONAL EVOLUTION

★ ★ ★

> *"To defend effectively, we must think like our adversaries, learn from every campaign, and strengthen every layer."*

## COMING NEXT IN PART III

**MITRE ATT&CK FRAMEWORK**
Understand adversary tactics.

**DETECTION ENGINEERING**
Build detections that work in the real world.

**THREAT HUNTING**
Proactively find threats before they strike.

III

PART III

# MITRE ATT&CK ANALYSIS & DETECTION ENGINEERING

ANALYZEDETECTDEFEND

*“Every observable behavior is an opportunity for detection.”*

CHAPTER 3

# MITRE ATT&CK FRAMEWORK

MITRE ATT&CK is a publicly available knowledge base describing how adversaries behave after gaining access to a target environment.

Unlike vulnerability databases, ATT&CK focuses on adversary behavior. It helps defenders answer questions such as:

- ✓ How did the attacker get in?
- ✓ What techniques were used?
- ✓ Where should detection occur?
- ✓ Which controls reduce risk?

**STRATEGIC OBSERVATION**

Mapping adversary behavior to ATT&CK tactics enables defenders to build targeted detections, inform response, and measure security posture across the attack lifecycle.

**ENTERPRISE ATT&CK TACTICAL FLOW**

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration
- Impact

# INITIAL ACCESS

The CERT-UA reports repeatedly identify phishing, exploitation of internet-facing services, and exploitation of known vulnerabilities as common entry vectors.

## COMMON ATT&CK TECHNIQUES

| ID | TECHNIQUE | DESCRIPTION | FREQUENCY |
|---|---|---|---|
| T1566 | Phishing | Spear phishing via email, malicious attachments or links. | ★★★★★ |
| T1190 | Exploit Public-Facing App | Exploitation of internet-facing web applications and services. | ★★★★☆ |
| T1133 | External Remote Services | Use of remote services such as RDP, VPN, or remote software. | ★★★☆☆ |
| T1078 | Valid Accounts | Use of legitimate accounts for initial access. | ★★★☆☆ |

## INDICATORS OF COMPROMISE

- Unexpected login locations
- Suspicious email attachments
- Abnormal VPN activity
- Authentication failures followed by success

## ANALYST NOTE

Phishing remains the most consistent initial access vector across all observed campaigns. User awareness and email security controls are critical.

# EXECUTION

After initial access, attackers execute payloads to establish control.

## FREQUENTLY OBSERVED METHODS

Office Docs → HTML/JS Payloads → Archive Files → Script Execution → Legit. Utilities

The H1 2023 report notes continued use of Office documents and HTML/JS-based delivery within compressed archives for execution.

## BLUE TEAM: MONITOR

- PowerShell
- Windows Script Host (wscript / cscript)
- cmd.exe
- mshta.exe
- rundll32.exe

## DETECTION FOCUS AREAS

- Process Creation Events
- Script Execution Logging
- File Download Monitoring
- Unusual Parent/Child Relationships
- Command Line Analysis

# PERSISTENCE

Persistence allows attackers to survive reboots and credential changes.

## COMMON PERSISTENCE TECHNIQUES

| TECHNIQUE | DESCRIPTION | EXAMPLES |
|---|---|---|
| Registry Run Keys | Modify registry keys to execute at user logon or system startup. | HKCU\Run, HKLM\Run, RunOnce |
| Scheduled Tasks | Create/modify tasks to run at specific times or events. | schtasks.exe, Task Scheduler |
| Services | Install malicious services that start with the system. | sc.exe create, New-Service |
| Valid Accounts | Use legitimate accounts for re-entry. | Domain Accounts, Local Accounts |
| Remote Admin Tools | Install RATs or remote access tools. | AnyDesk, RMM Tools, Custom RATs |

## BLUE TEAM: CHECKLIST

- ✓ Monitor startup folders and locations
- ✓ Monitor scheduled task creation & modification
- ✓ Monitor new or modified service creation
- ✓ Monitor registry modifications
- ✓ Monitor newly installed software and tools
- ✓ Review changes to remote access settings
- ✓ Correlate with user and system behaviour

## ANALYST NOTE

Attackers often combine multiple persistence mechanisms to maintain access even if one method is detected and removed.

# PRIVILEGE ESCALATION

Once inside a network, attackers frequently seek elevated privileges.

### TYPICAL OBJECTIVES

- Administrator accounts
- Domain admin
- Service accounts
- Backup operators


### HUNTING IDEAS — LOOK FOR:

- New administrator account creation
- Token manipulation or impersonation
- Credential dumping attempts
- Privileged logins outside normal hours
- Unusual group membership changes

### DETECTION STRATEGIES

- Monitor Privileged Logon Events
- Monitor Group Membership Changes
- Monitor UAC Bypass Attempts
- Monitor Use of Legitimate Tools
- Implement Least Privilege Access

# DEFENSE EVASION

Adversaries increasingly rely on legitimate tools and built-in system functionality to avoid detection and blend in with normal activity.

## LIVING-OFF-THE-LAND (LOTL)

Attackers abuse trusted utilities to achieve their objectives.

- **PowerShell** — scripting, execution, and automation
- **cmd.exe** — command execution and scripting
- **WMI** — system management and remote execution
- **WinRAR / 7-Zip** — archive creation and extraction
- **Windows Built-in Tools** — certutil, bitsadmin, mshta, regsvr32, schtasks, etc.

## DEFENDER ACTIONS

- Enable PowerShell logging (module, script block, transcription)
- Enable command-line auditing (process creation, command history)
- Deploy Sysmon (visibility into process, network, file events)
- Enable AMSI integration (detect malicious script content)
- Monitor LOLBAS usage (alert on unusual tool execution)
- Baseline normal activity (detect deviations and anomalies)

## STRATEGIC OBSERVATION

Blending in is the new stealth. Visibility into legitimate tool usage is now a primary defence requirement.

# CREDENTIAL ACCESS

Credential theft remains one of the most valuable objectives for adversaries, enabling broader access and privilege without exploiting new vulnerabilities.

## CREDENTIAL ACCESS LIFECYCLE

**1. Initial Access**
Foothold via phishing, exploit, or valid accounts

**2. Credential Harvesting**
Steal credentials from memory, browsers, keystrokes

**3. Credential Extraction**
Dump LSASS, registry, or other credential stores

**4. Credential Utilization**
Use or pass stolen credentials for lateral movement

## ATTACK EXAMPLES

| ID | TECHNIQUE | EXAMPLES |
|---|---|---|
| T1003 | Credential Dumping | Mimikatz, LSASS dumping |
| T1555 | Browser Credential Theft | Browser plugins, SQLite access |
| T1056 | Input Capture (Keylogging) | Keyloggers, screen capture |
| T1566 | Phishing | Spear phishing, fake login pages |

## DETECTION FOCUS

- LSASS access attempts
- Browser database access
- Unusual authentication patterns
- Multiple failed logins and brute force
- Credential use from unusual locations

## ANALYST NOTE

Once credentials are stolen, the attacker’s capabilities increase dramatically. Focus on early detection of credential access attempts.

# DISCOVERY

Before moving deeper, attackers map the environment to identify valuable assets, relationships, and potential attack paths.

## DISCOVERY ACTIVITIES

- Shared Folder Discovery
- Host Enumeration
- User Enumeration
- Software Inventory
- Network Scanning
- Domain Discovery

## HUNTING OPPORTUNITIES

- Repeated directory queries and file searches
- Internal network scanning and port discovery
- LDAP enumeration and Group Policy queries
- SMB enumeration and share discovery
- Rapid PowerShell reconnaissance commands

## STRATEGIC OBSERVATION

Discovery is noisy. Monitoring enumeration behaviours provides strong early indicators of adversarial activity.

# LATERAL MOVEMENT

Attackers rarely stop at the initially compromised system. They move laterally to reach high-value assets and critical systems.

## COMMON TARGET PATH

Initial Host → File Server → Domain Controller → Email Server → Database Server

| ID | TECHNIQUE | EXAMPLES |
|---|---|---|
| T1021 | Remote Services | RDP, WinRM, SMB |
| T1550 | Pass-the-Hash / Token Use | PtH, PtT, Overpass-the-Hash |
| T1078 | Valid Accounts | Domain admin, VPN users |
| T1027 | Windows Admin Shares | C$, ADMIN$ |
| T1047 | WMI | wmic, WinRM, WMI |

## DETECTION FOCUS

- New remote sessions from uncommon hosts
- Access to administrative shares
- RDP usage spikes or unusual patterns
- WinRM or WMI remote execution
- Lateral SMB traffic increases

## ANALYST NOTE

Lateral movement often precedes data theft or domain compromise. Early detection can prevent widespread impact.

# COLLECTION & EXFILTRATION

After achieving access, attackers collect valuable data and exfiltrate it using various methods, often within minutes of compromise.

## COLLECTION & EXFILTRATION FLOW

**1. Identify Valuable Data**
Locate sensitive documents, credentials, databases

**2. Collect & Stage Data**
Aggregate files and prepare for exfiltration

**3. Compress & Archive**
Compress data using ZIP, RAR, or other tools

**4. Exfiltrate Data**
Transfer data via C2, cloud, or other channels

## COMMON TARGETS

- Office Documents
- Email Archives
- Databases
- Browser Credentials
- Internal Reports
- Military Planning Docs

## DEFENDER PRIORITIES

- Data Loss Prevention (DLP) policies & monitoring
- Monitor outbound traffic and unusual destinations
- Alert on large archive creation & compression
- Detect cloud uploads and file transfers
- Monitor use of RAR, ZIP, 7z, and encryption tools

## STRATEGIC OBSERVATION

Exfiltration is the end goal. Monitoring data movement and volume anomalies is critical to stop adversaries before data leaves your environment.

# IMPACT

Not every campaign ends with destructive activity. Observed objectives vary depending on the operational intent of the adversary.


**Service Disruption**
Interrupt critical services and operational capabilities.

**Psychological Impact**
Create fear, uncertainty, reduce public confidence.

**Intelligence Collection**
Steal sensitive data, documents, credentials, communications.

**Data Destruction**
Wipe, corrupt, or encrypt data to cause long-term damage.

**Operational Delay**
Slow decision-making, degrade response, and cause disruption.

**STRATEGIC OBSERVATION**

Critical infrastructure campaigns may combine cyber activity with other forms of disruption, making resilience, redundancy, and rapid recovery essential.

# MITRE ATT&CK SUMMARY MATRIX

Prioritization aid for defenders based on themes recurring in analyzed reports.

| TACTIC | PRIORITY | RATIONALE |
|---|---|---|
| Initial Access | ★★★★★ | Phishing and exploitation are the most common entry vectors. |
| Execution | ★★★★☆ | Consistent use of documents, scripts, and LOLBins. |
| Persistence | ★★★★★ | Multiple persistence techniques observed in all campaigns. |
| Privilege Escalation | ★★★★☆ | Privilege abuse and token manipulation common. |
| Defense Evasion | ★★★★★ | Extensive use of LOLBins and anti-detection techniques. |
| Credential Access | ★★★★★ | Credential theft is a core objective across all actors. |
| Discovery | ★★★★☆ | Environment mapping is routine before movement. |
| Lateral Movement | ★★★★☆ | Movement to critical systems is consistently observed. |
| Collection | ★★★★★ | Rapid collection of valuable data is a recurring theme. |
| Command & Control | ★★★★☆ | C2 over HTTP/HTTPS and domain fronting observed. |
| Exfiltration | ★★★★★ | Data exfiltration follows collection within minutes to hours. |
| Impact | ★★★☆☆ | Destructive impact varies by campaign objective. |

### PRIORITY SCALE

★★★★★ Very High
★★★★☆ High
★★★☆☆ Medium
★★☆☆☆ Low
★☆☆☆☆ Very Low

### KEY TAKEAWAY

Focus detection on early tactics (Initial Access, Persistence, Credential Access) to reduce attacker success.

# SOC DETECTION PRIORITIES

Organize detection efforts based on risk and attacker behavior.

**TIER 1 — IMMEDIATE DETECTION**

- Phishing detection
- Suspicious logins
- Endpoint alerts
- Malware execution

**TIER 2 — ONGOING MONITORING**

- Credential theft
- PowerShell abuse
- Lateral movement
- Persistence changes

**TIER 3 — ADVANCED HUNTING**

- Threat hunting
- Behavioral analytics
- Long-term persistence
- Infrastructure-wide correlation

**STRATEGIC OBSERVATION**

Early detection stops attackers. Continuous detection reveals their intent. Hunting ensures we stay ahead of their next move.

# DETECTION ENGINEERING CHECKLIST

Layered visibility across the enterprise is key to successful detection.

### ENDPOINT

- ✓ Sysmon
- ✓ Windows Event Logging
- ✓ PowerShell Logging
- ✓ EDR / XDR
- ✓ Application Control
- ✓ Local Firewall

### IDENTITY

- ✓ MFA Enforcement
- ✓ Privileged Access Monitoring
- ✓ Authentication Analytics
- ✓ Password Policy Enforcement
- ✓ Service Account Monitoring

### NETWORK

- ✓ IDS / IPS
- ✓ DNS Monitoring
- ✓ Proxy Logs
- ✓ VPN Logs
- ✓ NetFlow / IPFIX
- ✓ Traffic Anomaly Detection
- ✓ Segmentation Monitoring

### EMAIL

- ✓ SPF, DKIM, DMARC
- ✓ Attachment Sandboxing
- ✓ URL Rewriting
- ✓ Phishing Simulation
- ✓ Email Gateway Filtering
- ✓ Threat Intelligence Feeds

### CENTRAL ANALYTICS

- ✓ SIEM Integration
- ✓ Log Correlation
- ✓ UEBA / Behavioral Analytics
- ✓ Case Management
- ✓ Threat Hunting Platform
- ✓ SOAR Automation

### BLUE TEAM PRINCIPLE

**Collect everything. Detect early. Respond fast. Improve continuously.**

END OF

# PART III

★ ★ ★ ★

## MITRE ATT&CK ANALYSIS & DETECTION ENGINEERING

> *"Detection is not about tools. It is about understanding behavior, asking the right questions, and seeing what others miss."*

### PREVIEW OF PART IV (PAGES 46-60)

The next chapter moves from tactics to the tools and software used during campaigns.

- Malware families (Remcos RAT, LummaStealer, MeduzaStealer, Remote Utilities, Cobalt Strike, Wipers)
- Initial access payloads
- Command-and-control patterns
- Malware lifecycle
- Indicators of Compromise (IOCs)
- YARA rule concepts
- Sigma detection concepts
- Malware comparison tables
- Defensive recommendations
- Case studies from CERT-UA reporting

# ABOUT THIS HANDBOOK

This handbook is a defensive resource designed to enhance understanding of cyber threats and strengthen the collective ability to build secure, resilient, and trusted digital environments.

**KNOWLEDGE IS DEFENCEPREPAREDNESS IS RESILIENCEUNITY IS STRENGTH**

This material is intended for authorized professionals, researchers, students, and organizations committed to cybersecurity, national security, and the protection of digital society.

FOR DEFENSIVE & EDUCATIONAL USE ONLY

ROHIT DINDE • FIRST EDITION • 2026