THE HUNTER BECOMES THE HUNTED

Protecting High-Value Research from Nation-State Espionage

"Security researchers used to chase attackers. Today attackers chase researchers."

Dr Erdal Ozkaya

- CISO @Morgan State University
- President of Global CISO Forum
- 100 + Industry Certification
- Author 26 published books & many Security Certifications & Courseware

Dr. Erdal Ozkaya

C|EH HALL OF FAME 2021

Microsoft REGIONAL DIRECTOR

Cisco Champion

MVP Microsoft Most Valuable Professional

CEI of the Year EC-Council

EC-Council Excellence

My Books

DR ERDAL OZKAYA

Translated


网络安全与
攻防策略
现代威胁应对之道


Кибербезопасность:
стратегии атак и обороны


SİBER
GÜVENLİK


金融网络安全


Cyberbezpieczeństwo
Strategie ataku i obrony
Packt


İnternet ve Telefon
Dolandırıcılığı:
Sosyal
Mühendislik
seçkin

The Strategic Shift

2010

BREAK IN

2026

LOG IN

Adversaries no longer need to exploit your OS;

they simply exploit your session.

The Awakening

The Core Paradox

Your greatest breakthrough **is also your greatest liability.**

The knowledge you hold — **0-days, proprietary tools, client intelligence, unpublished CVEs** — is worth millions to adversaries.

The shift has happened:
From 'Breaking In' → To 'Logging In'

312%
increase in researcher targeting

$4.2M
avg value of stolen research IP

7
nation-state groups actively targeting labs in 2026

Why Researchers Matter

"Researchers hold cyber weapons before anyone else."

- **Zero-Day Repos:** High-value unpatched vulnerabilities.
- **Detection Logic:** Blueprints for defensive tools.
- **Exploit PoCs:** Functional code ready for weaponization.
- **Threat Intel:** Aggregated data on adversary movements.

Who's Coming For You

LAZARUS GROUP

REGION: DPRK

PRIMARY TARGETS

Crypto research, exploit brokers, vuln hunters

TTPs

LinkedIn personas, fake job offers, trojanized tools

COZY BEAR

REGION: Russia / SVR

PRIMARY TARGETS

Policy researchers, cloud security teams

TTPs

Supply chain poisoning, OAuth abuse, session hijacking

APT41

REGION: China / MSS

PRIMARY TARGETS

Vulnerability researchers, red team operators

TTPs

AI-driven spear-phish, weaponized VSCode extensions

The Real Target: Expanded Lab

GitHub

Private repos containing sensitive toolchains and fuzzing logic.

Slack / Comms

Internal discussions on active hunts and client vulnerability reports.

Cloud Lab

Compromised VMs and staging environments for exploit testing.

Personal Laptop

The gateway to the lab — often the weakest link in the chain.

Conf Laptop

High-exposure hardware used in adversarial environments.

Identity

The goal: session tokens and browser-cached credentials.

Your research isn't just a byproduct; it's a nation-state primary objective.

If they own the researcher, they own the defenses of the next decade.

DR ERDAL OZKAYA


THE ADVERSARY
Understanding the state-sponsored targeting cycle.
DR ERDAL OZKAYA

Who's Coming For You

LAZARUS GROUP

REGION: DPRK

PRIMARY TARGETS

Crypto research, exploit brokers, vuln hunters

TTPs

LinkedIn personas, fake job offers, trojanized tools

COZY BEAR

REGION: Russia / SVR

PRIMARY TARGETS

Policy researchers, cloud security teams

TTPs

Supply chain poisoning, OAuth abuse, session hijacking

APT41

REGION: China / MSS

PRIMARY TARGETS

Vulnerability researchers, red team operators

TTPs

AI-driven spear-phish, weaponized VSCode extensions

The Nation-State Playbook

RECON	SOC ENG	IDENTITY	ACCESS	THEFT
Profiling researchers via GitHub & Talks.	Deepfake calls & collab requests.	AiTM & token theft execution.	Persistent stealth lab monitoring.	Exfiltration of 0-day research.

Attack Vector #1: Session Token Theft

01

Initial Recon

Target's cloud tools and browser environment identified via OSINT

02

Malicious Payload

Trojanized npm package, browser extension, or PDF with embedded JS

03

Token Extraction

Session cookies and OAuth tokens exfiltrated silently to C2 server

04

Persistent Access

Adversary logs in as you — bypassing MFA entirely. Dwell begins.

⚠ **MFA does NOT protect against session token theft — the attacker uses your authenticated session, not your password**

Attack Vector #2: Weaponized Cloud Tooling

WEAPONIZED ATTACK SURFACES

VSCode Extensions

Malicious marketplace extensions exfiltrate code and credentials on save

GitHub Actions

Poisoned CI/CD workflows that capture secrets during build pipelines

Cloud IDE Plugins

Compromised Copilot-style tools sending code to adversary infrastructure

npm / PyPI Packages

Typosquatted packages targeting researcher dependencies

Docker Images

Backdoored base images in public registries used in lab environments

THE INSIGHT

"The tools you rely on to do your research have become the attack surface."

Adversaries now invest heavily in the developer toolchain ecosystem — the same environment researchers use daily. They understand that a researcher who trusts their tools implicitly will never question why their IDE plugin needs network access.

Attack Vector #3: AI-Driven Social Engineering

REAL ATTACK SCENARIO — 2026

A researcher receives a LinkedIn message from 'Dr. Sarah Chen, Senior Research Engineer at Google Project Zero.' The profile has 500+ connections, 3 years of history, published papers, and a verified-looking email. She proposes collaboration on an upcoming research project. The video call is flawless. The follow-up includes a shared repository. Everything checks out — until the repository contains a malicious tool.

Synthetic Personas

AI-generated researchers with years of fake publication history, social graphs, and deepfake video call capability

Hyper-Personalized Phishing

LLMs trained on your public writing, GitHub commits, and talks to craft lures indistinguishable from trusted contacts

Voice & Video Cloning

Real-time deepfake audio/video of known colleagues, conference calls with 'your manager' requesting urgent access

Reconnaissance: You Are Leaking

GitHub

Revealing your tech stack and current research focus via commits.

LinkedIn

Mapping your professional network for targeted social engineering.

Papers

Demonstrating your deep expertise to invite "peer" collaboration.

"Researchers leak reconnaissance data about themselves every day."

Scenario: Deepfake Social Engineering

The Impersonation

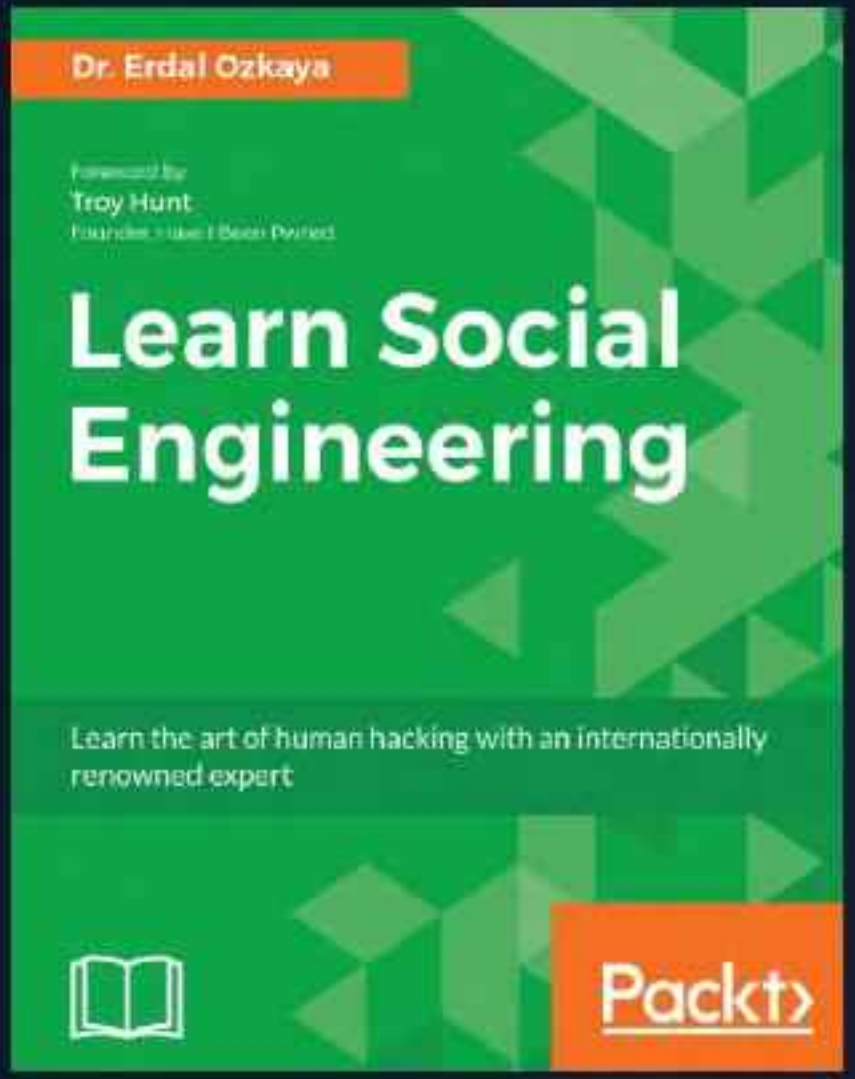
Attacker clones the voice of a known **Conference Organizer** or a senior **Microsoft Engineer** .

"Hey, we've reviewed your submission. We need to jump on a quick call to discuss the staging environment."

The "Actionable" Request

During a deepfake video/voice call, the attacker provides a "Secure Collaboration Link" (AiTM Proxy).

"Just login here to sync your repo with our testing lab."




STRONTIUM attack case study


Government Target
Diplomatic Organization
Government Target
Government Target
Government Target
Government Target
STRONTIUM Attacks
Attempts
Confirmed Infection
UNITED KINGDOM
DENMARK
Copenhagen
Riga
Minsk
BELARUS
GERMANY
Amsterdam
Berlin
Warsaw
POLAND
Kyiv
UKRAINE
FRANCE
Paris
AUSTRIA
HUNGARY
Budapest
Ljubljana
Zagreb
ROMANIA
Chișinău
ITALY
Rome
SPAIN
Lisbon
PORTUGAL
Sofia
Podgorica
Tirana
GREECE
TURKEY
KAZAKHSTAN
Caspian Sea
GEORGIA
SYRIA
IRAQ
IRAN
AFGHANISTAN
INDIA
MOROCCO
TUNISIA
ALGERIA
LIBYA
EGYPT
NIGER
SAUDI ARABIA
OMAN
YEMEN
Red Sea

TARGET: Diplomat in the Middle East

From: <attacker>@<email provider.com>
To: <victim>@<email provider.com>
Subject: Re: Mission In Central African Republic

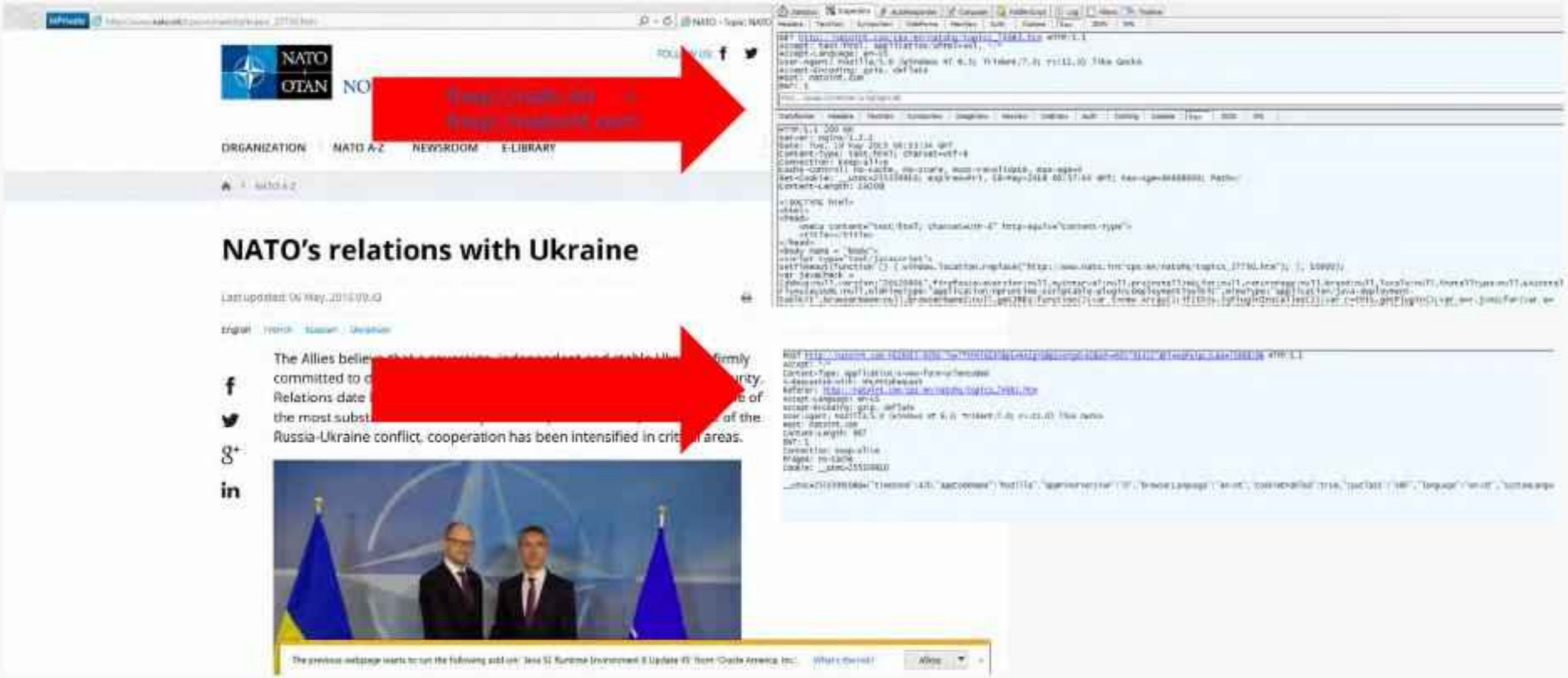
Dear Sir!
Please be advised that The Spanish Army personnel and a
currently deployed in the Central African Republic (CAR) a
European EUFOR RCA mission will return to Spain in early

Visit
hxxp://eurasiaglobalnews.com/9067011?-spains-armed
for the addition info.

Best regards,

*Capt. <omitted>, Defence Adviser, Public Diplomacy Div
provider.com>

TARGET: NATO-Themed Spear Phish



ATTACK: Stages of a 0-day Attack

1

Initial Exploit URL (Flash 0day)

TimeStamp	Alert	Data
2015/04/08 10:11:54	Unknown URL Report	hxxp:militaryadviser.org/hu/press-center/news/426728-ukraine/440136/

2

Kernel Mode Exploit (0day)

TimeStamp	Alert	Sha1	FileName	Parent Process
2015/04/08 10:12:11	Win32/ContextualDropIETemp	b22233684bc8aa939629f4cbebb18545c7121548	runrun.exe	iexplore.exe

3

Stage 1: Backdoor

TimeStamp	Alert	Sha1	FileName	Parent Process
2015/04/08 10:12:11	#LowFiContextRundllAppdata	ef1a7b1a92b7b00f77786b6a1bffc4e495ccf729	odserv.dll	rundll32.exe

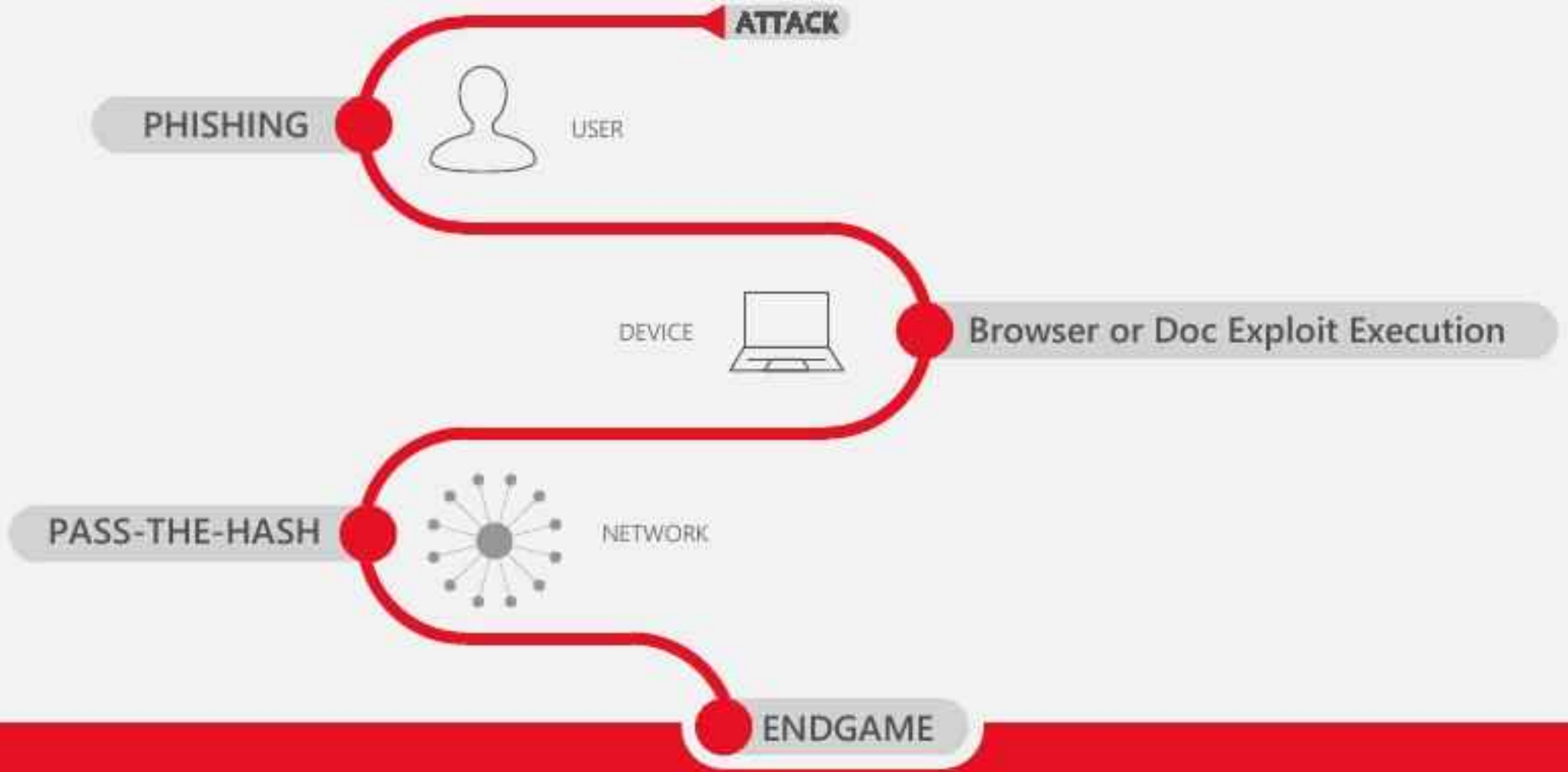
4

Stage 2: Pass-the-Hash Module

TimeStamp	Alert	Sha1	FileName	Parent Process
2015/04/09 06:34:04	#HackTool:Win32/WDigest.A!dha	ca709ec79ee0518b77f161bc8bab8847c889cb88	psw.exe	rundll32.exe

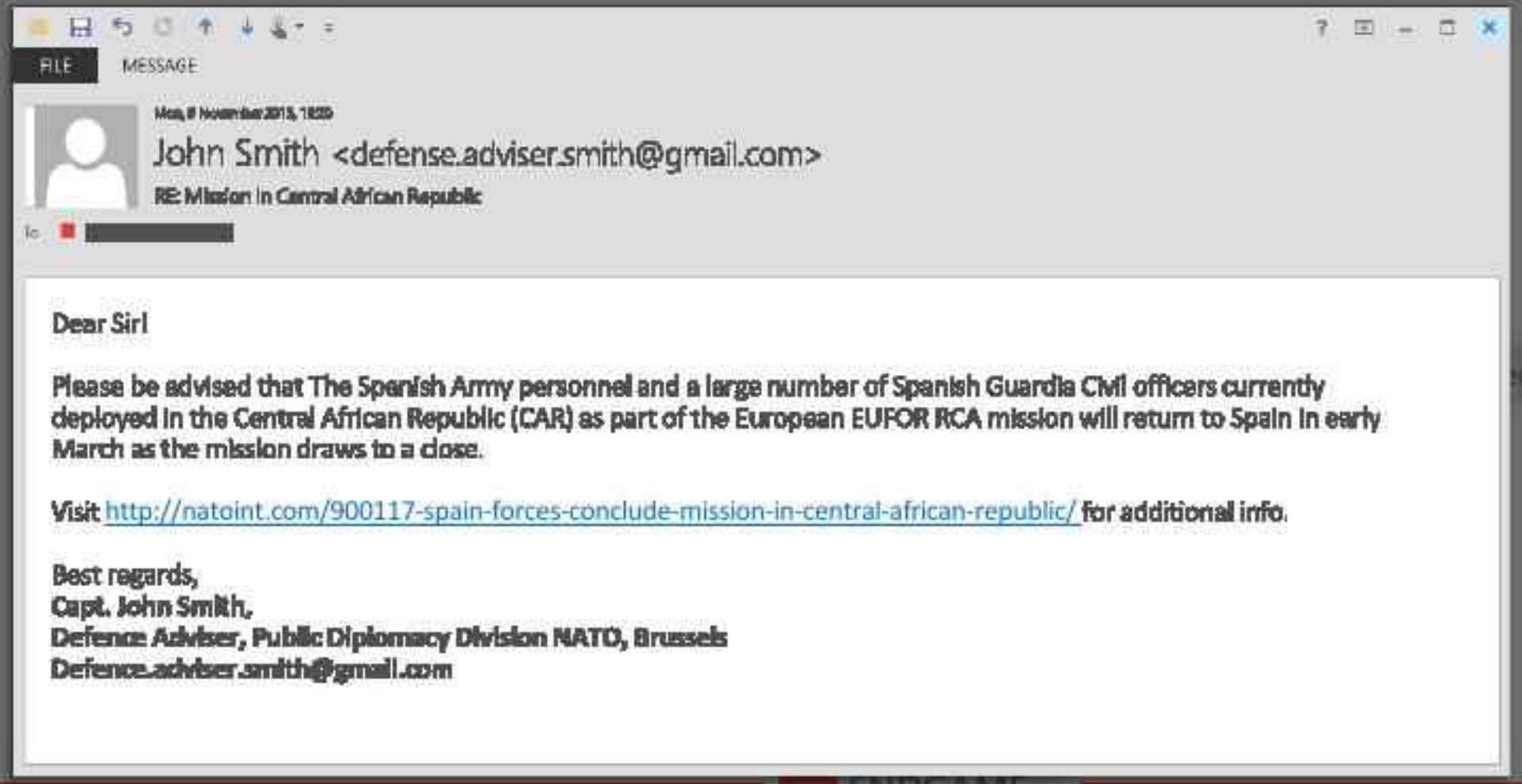
ANATOMY OF AN **ATTACK**

ANATOMY OF AN **ATTACK: STRONTIUM**



Theft of sensitive information, disruption of government.

ANATOMY OF AN **ATTACK: STRONTIUM**



ENDGAME

Theft of sensitive information, disruption of government.

ANATOMY OF AN **ATTACK: STRONTIUM**

ATTACK

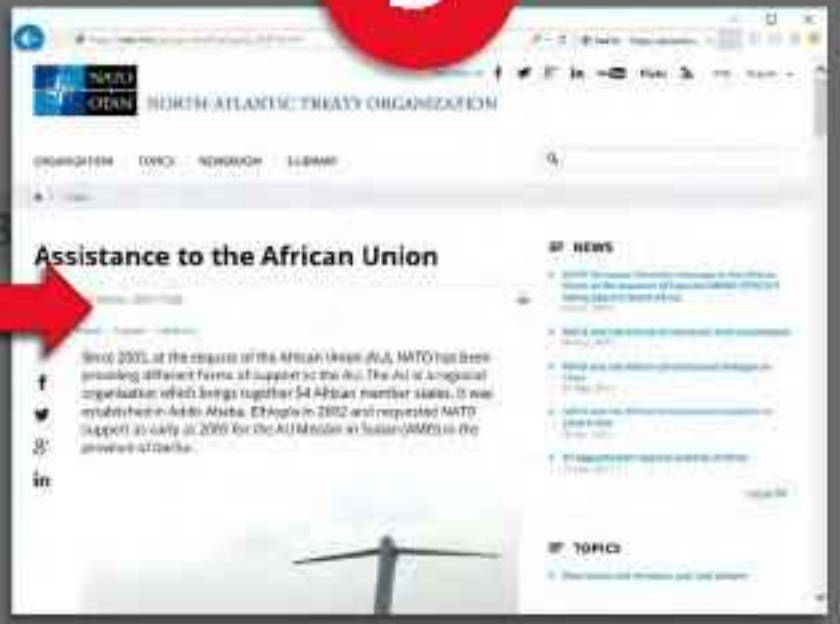
1 PHISHING

2

3

Land on exploit page

Exploit runs



Redirected to legitimate page

ENDGAME

Theft of sensitive information, disruption of government.

COMPROMISING THE LAB

Technical deep dive into current attack flows.

Attack Flow: Token Theft

01	02	03	04	05
Phishing Email with Proxy Link	*Credential Capture (Username/Pass)*	Extraction of Session Cookie	Token Replay on Attacker Device	Full GitHub / Lab Access

MFA protects the LOGIN. MFA does NOT protect the ACTIVE SESSION.

Why Token Theft Wins

What MFA Protects

- ✓ Initial Authentication
- ✓ Credential Replay
- ✓ Password Guessing

What MFA Ignores

- ✗ Session Cookie Reuse
- ✗ Reverse Proxy (AiTM)
- ✗ Stolen Auth Tokens

Weaponized: Browser Infostealers

RedLine / Vidar

Standardized malware for bulk cookie extraction.

Lumma / RisePro

Advanced stealth-focused stealers targeting dev tools.

The Prize

GitHub PATs, AWS Keys, and Chrome Session Databases.

GitHub: The Central Target

Exploit PoCs: The liquid gold of the researcher lab.

Fuzzing Tools: Your proprietary logic for finding bugs.

Unreleased Reports: Vulnerability data before it goes to the vendor.

Research Supply Chain Poisoning

Your "defensive tools" are becoming "offensive gateways."

CROWN JEWEL FRAMEWORK

Applying CISO governance to researcher data.

THE CISO QUESTION:

"WHAT WOULD AN ADVERSARY STEAL FIRST?"

Crown J ewels Framework

EYES ONLY

Live exploits, 0-days, client reports under NDA

CRITICAL

Unpublished CVEs, proprietary tools, pentest findings

SENSITIVE

Research notes, tool source code, collaboration details

PUBLIC

Published papers, blog posts, public repos

IDENTIFICATION QUESTION:

Ask of every asset — 'If this data were in an adversary's hands tomorrow, what's the blast radius?'

Research Data Mapping

// DATA FLOW PATHWAY

1. Research Workstation
2. GitHub Enterprise / Private Repos
3. Cloud Lab Staging
4. Shared Data Lake / Fuzzing Results
5. Final Report Drafts (Client Vault)

RESEARCH OPSEC FRAMEWORK

The core defensive model for modern security teams.

OPSEC Countermeasures

01

Identity & Session Management

- FIDO2/Passkeys — phishing-resistant, device-bound auth
- Short-lived token policies (15-min max for sensitive systems)
- Browser profile isolation per research project

02

Environment Isolation

- Air-gapped VM for Crown Jewel research
- Separate hardware for internet-facing tools
- Zero-trust network segmentation in the lab

03

Supply Chain Hygiene

- Private package registry with verified packages only
- Extension allowlist enforcement in VSCode
- Egress monitoring from all development environments

04

AI Social Engineering Defense

- Out-of-band verification for all new collaboration requests
- Code word protocol with known colleagues before sharing
- Deepfake detection checklist for video calls

The Research OPSEC Model

Defensive Layers

1. **Identity Security:** The foundation of access.
2. **Environment Security:** Hardening the workspace.
3. **Data Protection:** Encrypting the crown jewels.
4. **Monitoring:** Observing behavioral anomalies.
5. **Response:** Rapid containment of token theft.

Research OPSEC Framework

TOP 5 ACTIONS — THIS WEEK

1. Map your Crown Jewels — classify every active research asset this week
2. Deploy FIDO2/passkeys for all systems touching sensitive research data
3. Audit every VSCode extension, npm package, and cloud integration in your lab
4. Establish out-of-band verification protocol for new collaboration requests
5. Run a researcher-compromise tabletop exercise with your leadership team

THE MINDSET SHIFT

"Stop asking: Am I a target?

Start asking: What would my adversary want most from me today — and is it protected?"

Research OPSEC is not paranoia.
It is professional hygiene.


THREAT HUNTING
Proactively finding the adversary in the lab
DR ERDAL OZKAYA

Espionage Indicators (IoBs)

Midnight Access

Logins between 01:00 and 04:00 local time.

Mass Cloning

User account cloning >10 private repos in <5 minutes.

New Tokens

Creation of Personal Access Tokens without a Change Request.

Example Hunt Query: GitHub

```
SELECT user, action, data_size,
src_ip
  FROM github_audit_logs
  WHERE action = 'repo.clone'
  AND data_size > 5GB
  AND device_id NOT IN (known_devices)
  AND auth_method = 'token'
```

Detecting high-volume exfiltration via stolen PATs.

REAL CASE STUDIES

Learning from the front lines of research espionage.

CASE STUDY: THE LAZARUS RAPPORT

// TARGET: THE SECURITY COMMUNITY

Strategic Rapport Attacks

The Lazarus Group (Diamond Sleet) executed a multi-year campaign (2021-2024) specifically targeting vulnerability researchers.

- **Persona Aging:** High-credibility Twitter/X and LinkedIn profiles built over months.
- **Collab Lure:** Sending malicious Visual Studio projects for "joint research."
- **Payload:** Custom DLLs executed via build events in VS Projects.

CASE STUDY: APT29 IDENTITY THEFT

IdP Targeting

Midnight Blizzard (APT29) targets Cloud Identity Providers (Entra ID) to harvest OAuth tokens and session cookies.

OAuth Persistence

Granting malicious "Research Tool" apps permanent access to private GitHub and Microsoft 365 environments.

Tenant Pivot

Using one compromised researcher account to move laterally into high-value corporate tenants.

CASE STUDY: OPERATION DREAM JOB

75%

Increased AI Credibility

// PHANTOM RECRUITING CAMPAIGN

Targeted Fake Interviews

State-sponsored actors impersonate HR from high-tier tech firms (Google, Microsoft) to target security researchers.

- **Weaponized JD:** Malicious "Job Description" PDFs containing infostealer payloads.
- **Deepfake Calls:** AI-generated voices used for pre-interview screening calls.
- **Technical Test:** Delivering malicious ISO files as "coding assignments."

IF ATTACKERS STEAL

THE RESEARCH...

THEY STEAL

TOMORROW'S DEFENSES.

DR ERDAL OZKAYA

Dankie Faleminderit Shukran Chnorakaloutioun Hvala شكرًا لك Blagodaria

Děkuji Tak Bedankt Tänan Kiitos Merci Danke Ευχαριστώ A dank

Mahalo .תודה Dhanyavād Köszönöm Takk Terima kasih Grazie Grazzi

Thank you!

DR ERDAL OZKAYA

감사합니다 Paldies Choukrane Ačiū Благодарам ありがとうございました

谢谢 Баярлалаа Dziękuję Obrigado Mulţumesc Спасибо Ngiyabonga

Ďakujem Tack Nandri Kop khun Teşekkür ederim Дякую Хвала Diolch

Keep in Touch

@DrErdalOzkaya

Dr Erdal Ozkaya

www.ErdalOzkaya.com

@drerdalozkaya

https://www.youtube.com/erdalozkaya