Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

CrypTO CONFERENCE

Politecnico di Torino 1859
Telsy A TIM ENTERPRISE BRAND
DISMA

CROWDSTRIKE

Follow the **(crypto) money**

2025 CrypTO Conference

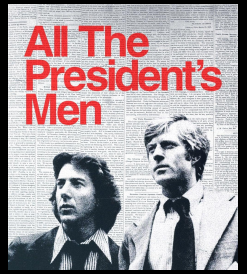
Alessandro Guggino

whoami

Alessandro Guggino
Senior Security Researcher
CrowdStrike

- BS & MS in Computer Engineering at **Politecnico di Torino**
- Formerly R&D at **BitPolito**, **LINKS Foundation**
- Counter Adversary Operations / Cyber Intelligence R&D at **CrowdStrike**

Follow the money



All The President's Men

1976 movie by A. Pakula

Agenda

01 ROYAL SPIDER Profile

02 Ransomware Operation

03 Bitcoin Tracing

04 Key Findings

ROYAL SPIDER

Origins

Russian Federation
🇷🇺

Type

eCrime – Financially Motivated

First seen

September 2022
(still active)

Malware

Ransomware-as-a-Service:
Royal, BlackSuit

Ransomware Operation

Infection

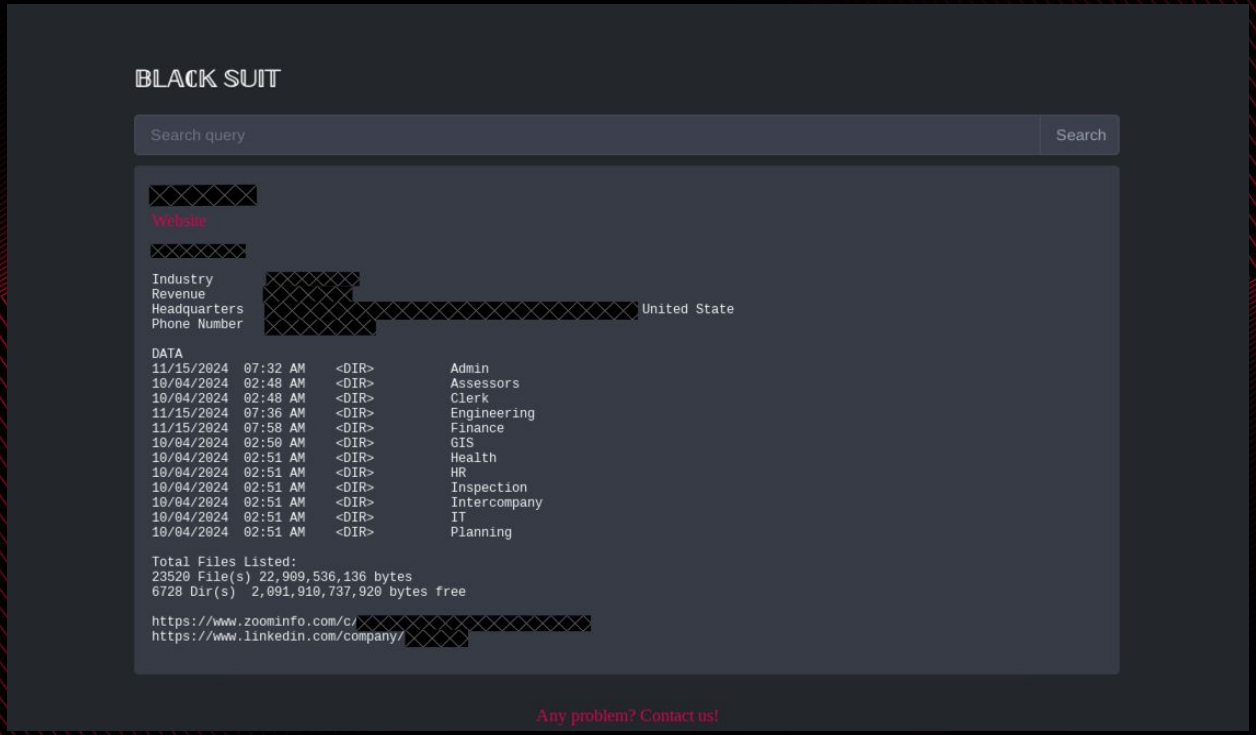
Exfiltration

Encryption

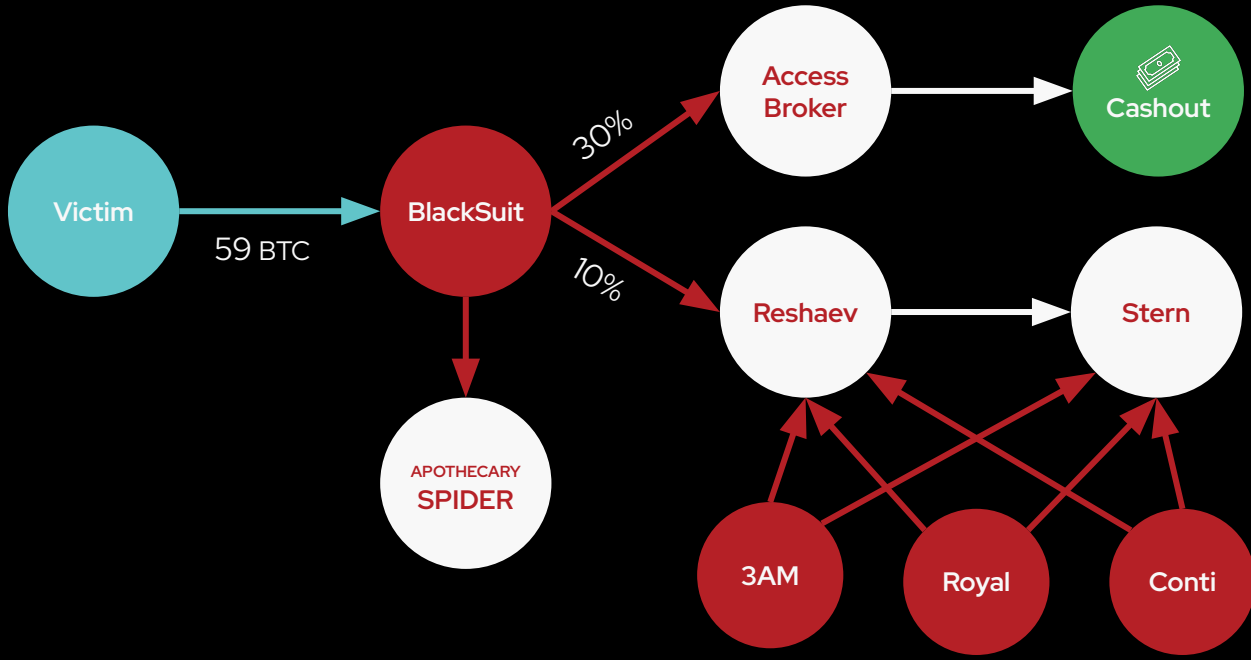
Ransom demand

Money distribution and laundering

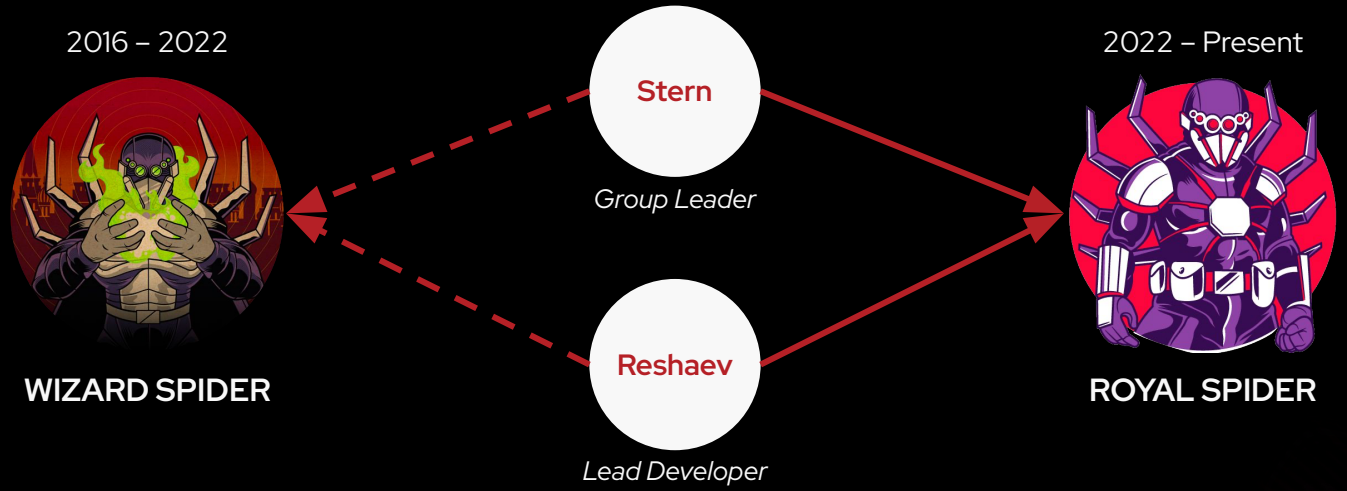
Dedicated Leak Site



Case: Bitcoin Tracing



Case: Bitcoin Tracing



REWARD UP TO $10 MILLION

FOREIGN GOVERNMENT-LINKED MALICIOUS CYBER ACTIVITY TARGETING U.S. CRITICAL INFRASTRUCTURE

If you have information that ties hacking groups such as Conti, TrickBot, Wizard Spider; the hackers known as “Tramp,” “Dandis,” “Professor,” “Reshaev,” or “Target”; or any malware or ransomware to a foreign government targeting U.S. critical infrastructure, you may be eligible for a reward.

Send your information to RFJ via our Tor-based tip line below.

Tor Link:he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion

U.S. Department of State
Diplomatic Security Service
Rewards for Justice

+1-202-702-7843
@RFJ_USA

rewardsforjustice.net/rewards/conti

CROWDSTRIKE

Key Findings

- **Stern and Reshaev** (former **WIZARD SPIDER** members) involvement in **ROYAL SPIDER**
- **BlackSuit = Royal Ransomware**
- **ROYAL SPIDER affiliates** usage of **IABs** and **Loaders**
- Usage of **Exchanges** and **Money Laundering services**

Thank you!

Alessandro Guggino

Senior Security Researcher

alessandro.guggino@crowdstrike.com