Scale, Sophistication, Speed: Navigating the Modern Threat Landscape

André Reichow-Prehn
Managing Partner
EMEA and LATAM, Unit 42

September 2024

Palo Alto Networks Unit 42

Proactive Services

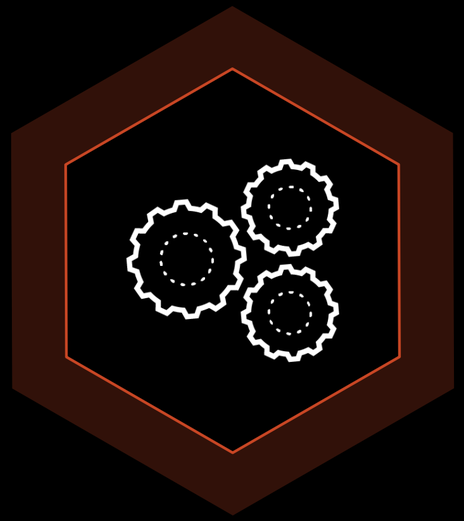
Managed Services

Incident Response

Threat Intelligence

The Threat Landscape Is Intensifying

Scale



Sophistication

Speed

$8 TRILLION

COST OF CYBERCRIME

Scale

Vulnerabilities Surpass Phishing as Most Common Initial Attack Vector

MOVEit

2,176

exposed devices

Estimated 8K victims globally

Citrix Netscaler

108,810

exposed devices (Citrix ADC and Gateway)

Atlassian Confluence

102,686

exposed devices

Cisco IOS XE

2,110

exposed devices

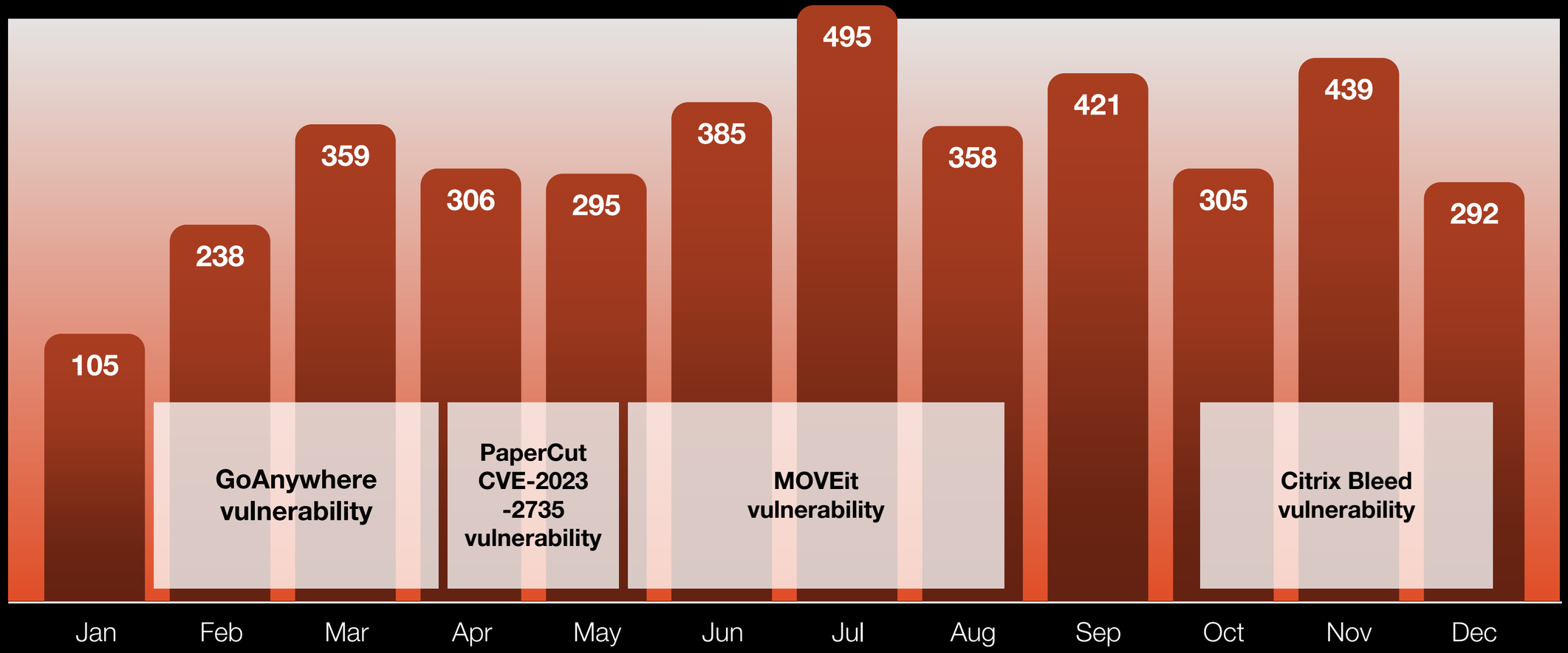
Policy Secure Connect Secure

28,474

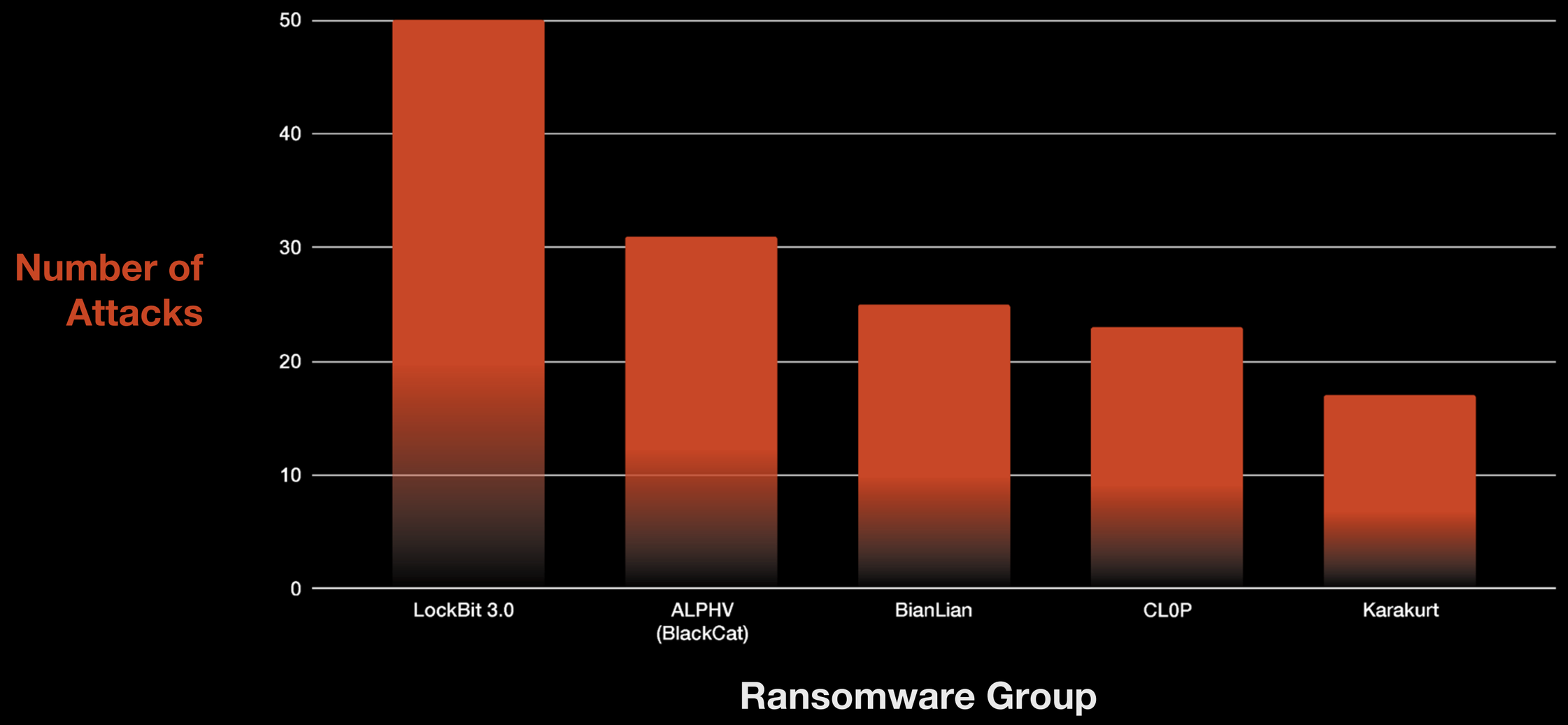
exposed devices

The Scale of Ransomware Attacks Is Up 50% YoY

2023 Leak Site Posts From Ransomware Groups, by Month

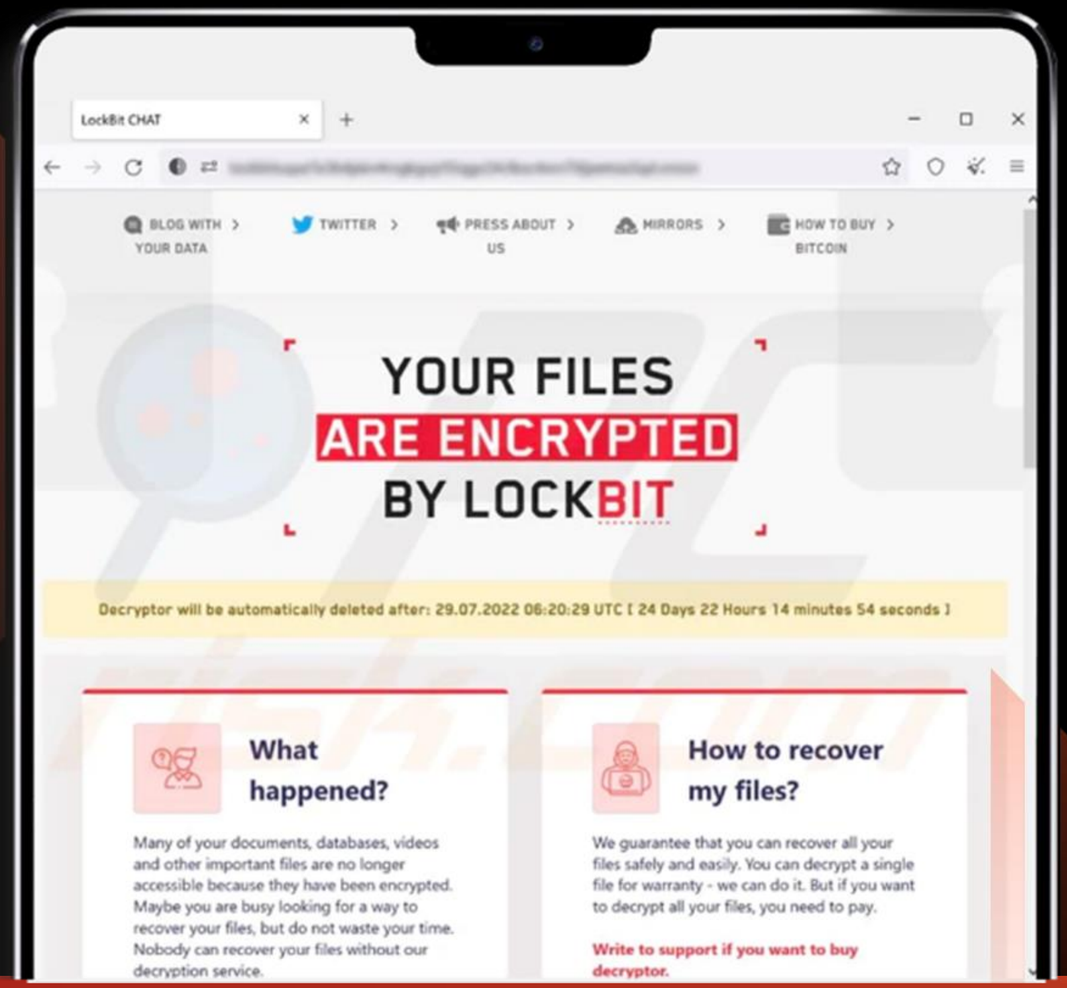


Top Groups



Public postings on leak sites tracked by Unit 42, January-December 2023

LockBit – Down But Not Out



LE takedown Feb. 19, 2024.

LockBit's own operations compromised by PHP vulnerability.

Relaunched infrastructure Feb. 24.

Updated ransom notes

Same tooling

47%

Decrease in leak site posts for comparable periods in 2023 and 2024.

Announced dedicated targeting of .gov, .edu, .org

– But post-takedown leaks show every industry affected

Sophistication

What’s in a name? Muddled Libra

WHO

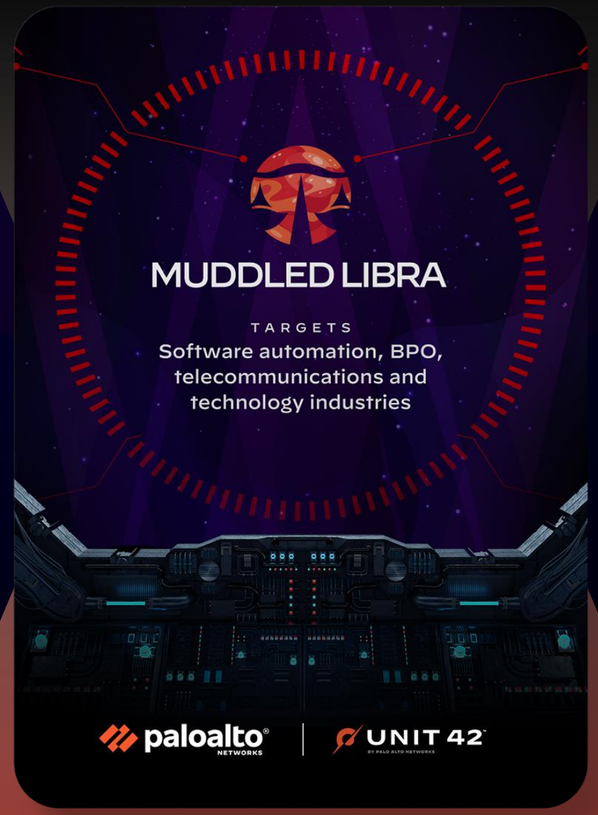
Origin
- Social Chat
- Gaming Groups

Numbers
- Thousands Strong
- Few Consequential

Geography
- Primarily NA
- Few Europe

Language
- Fluent English

Organization
- AlphV Affiliate
- Agile Teams



HOW

Key Tactics
- MFA Bypass
- Social Engineering

Proficiencies
- SaaS / Cloud
- OSINT

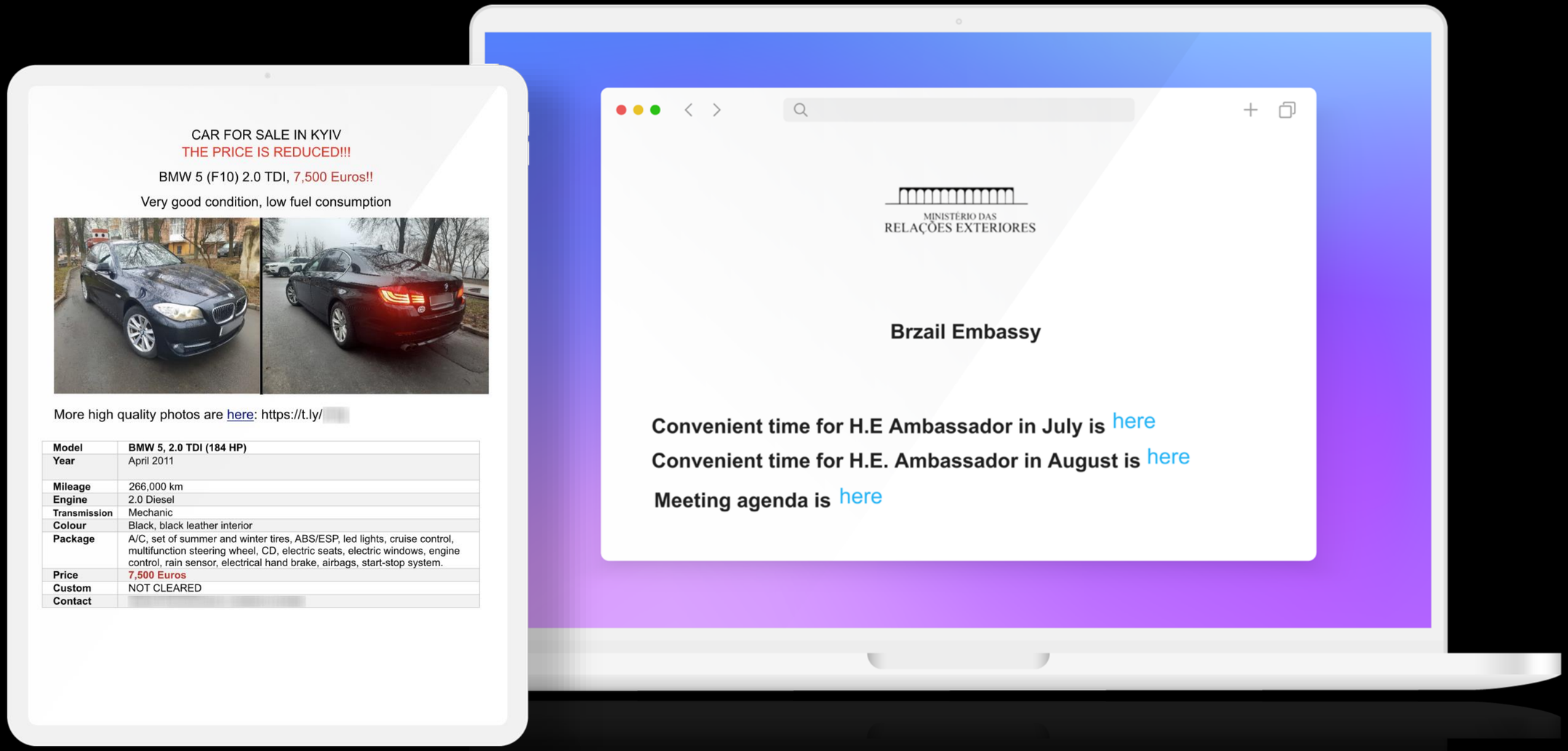
Tradecraft
- LOLBINs
- RMMs
- Blackcat

Campaigns
- Industry Clustering

Objective
- Extortion
- Data Theft
- Disruption

Creativity is Reaching a New Level

Cloaked Ursa (Russia)



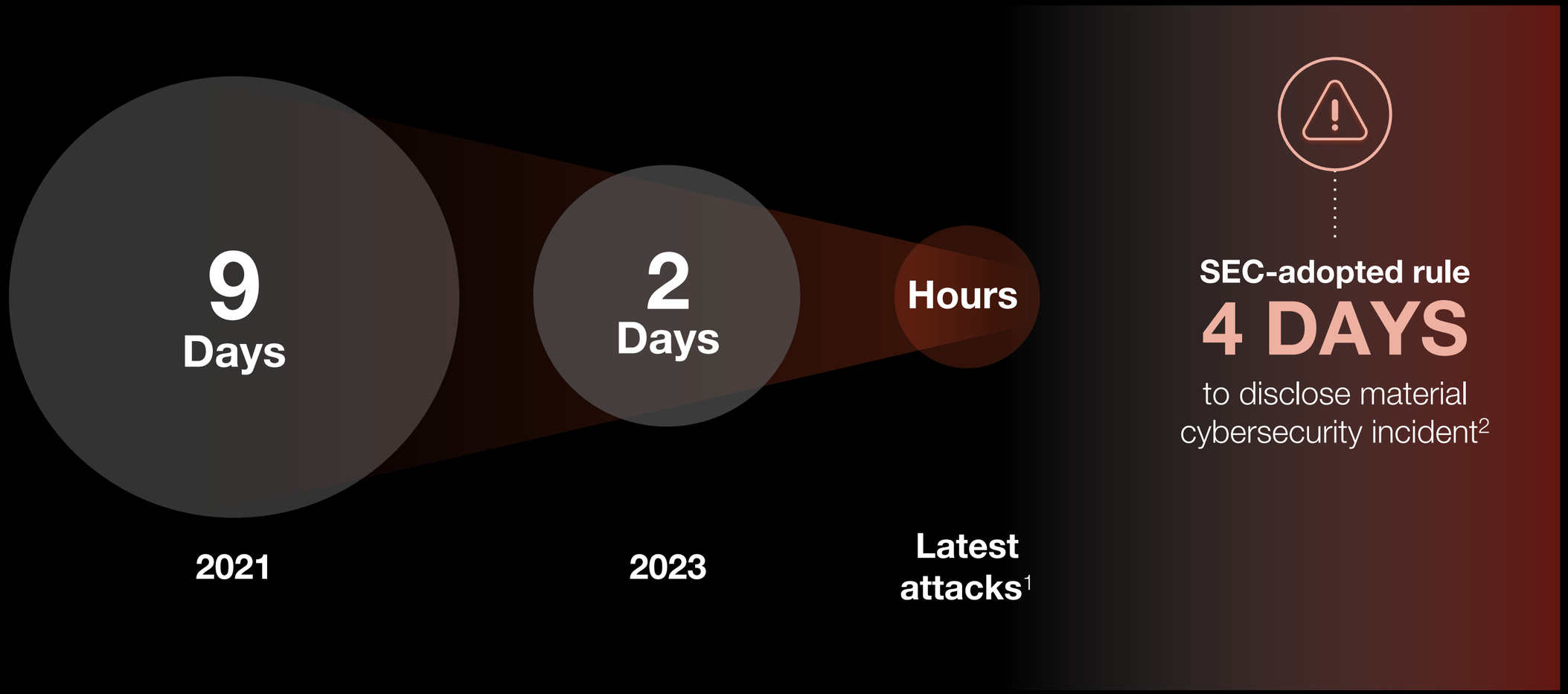
APTs are Targeting Job Applicants and Companies

DPRK (North Korea)

Speed

Attacks Happening Faster Than Organizations Can Respond

Median Days From Compromise to Exfil (MTTE)



[1] Source: Unit 42 IR data. [2] SEC rule: Report “material” cybersecurity incidents on a Form 8-K within four business days of materiality determination.

Actors Move at Machine Speed To Exploit New Vulnerabilities

[1] Source: Unit 42 IR data.

3 waves of attacks

5 vulnerabilities in less than 30 days – affecting 145 countries worldwide

Government agencies worldwide issued warnings:

- **CISA (U.S.)**
- **ASD's ACSC (Australia)**
- **NCSC-UK**
- **Canadian Centre for Cyber Security**
- **NCSC-NZ**

UNIT 42
BY PALO ALTO NETWORKS

Assess

Proactive Assessments to **test and validate your security controls against the right threats**

- Ransomware Readiness Assessment
- Compromise Assessment
- Red & Purple Team / Pentest Exercises
- Incident Response Plan Development & Review
- Cloud Security Assessment
- Tabletop Exercises
- Breach Readiness Review
- SOC Assessment
- Supply Chain Risk Assessment
- Business Email Compromise Readiness Assessment

Evolve

Strategic Advisory services to help **evolve your security strategy with a threat-informed approach**

- BoD Security Strategy Review
- Security Program Design
- Cyber Risk Assessment
- Virtual CISO
- M&A Cyber Due Diligence

Respond

Incident Response & investigation services to **mobilize your response and recovery**

- Business Email Compromise
- Ransomware Investigation
- APT Investigation
- PCI Investigation
- Cloud Incident Response
- OT/ICS Incident Response
- Web App Compromise
- Digital Investigations & Insider Threat
- Mobile Forensics
- Structured Data Investigations
- Expert Witness / Testimony / Litigation Support

Unit 42 Retainer

A prepaid block of credits that can be used for Incident Response or for any of our Proactive Services

paloalto NETWORKS | UNIT 42