LRQA NETTITUDE

Vital steps to become ransomware resilient

Jamie Roderick

Head of Cyber Incident Response

LRQA Nettitude

Leadership Series

Agenda

01 Ransomware evolution

02 Ransomware in 2023

03 Implementing resilience

04 Questions

Ransomware Evolution

1

Leadership Series

Ransomware actors

A selection of actors with attributed ransomware operations:

Russian-nexus/state-sponsored

- Sandworm (2017 - NotPetya)
- Conti, Evil Corp

Criminal

- Fluid and evolving groups: LockBit 3, REvil Gang, Maze, Darkside, Ryuk, Babuk, Clop, Royal, PLAY, BlackCat, BianLiam, BlackBasta
- New(ish) groups: Medusa, AKIRA, 8Base

China

- APT27, Emissary Panda (2020 to date)
- HAFNIUM (2020)
- APT41, Wicked Panda (2019 – 2020)

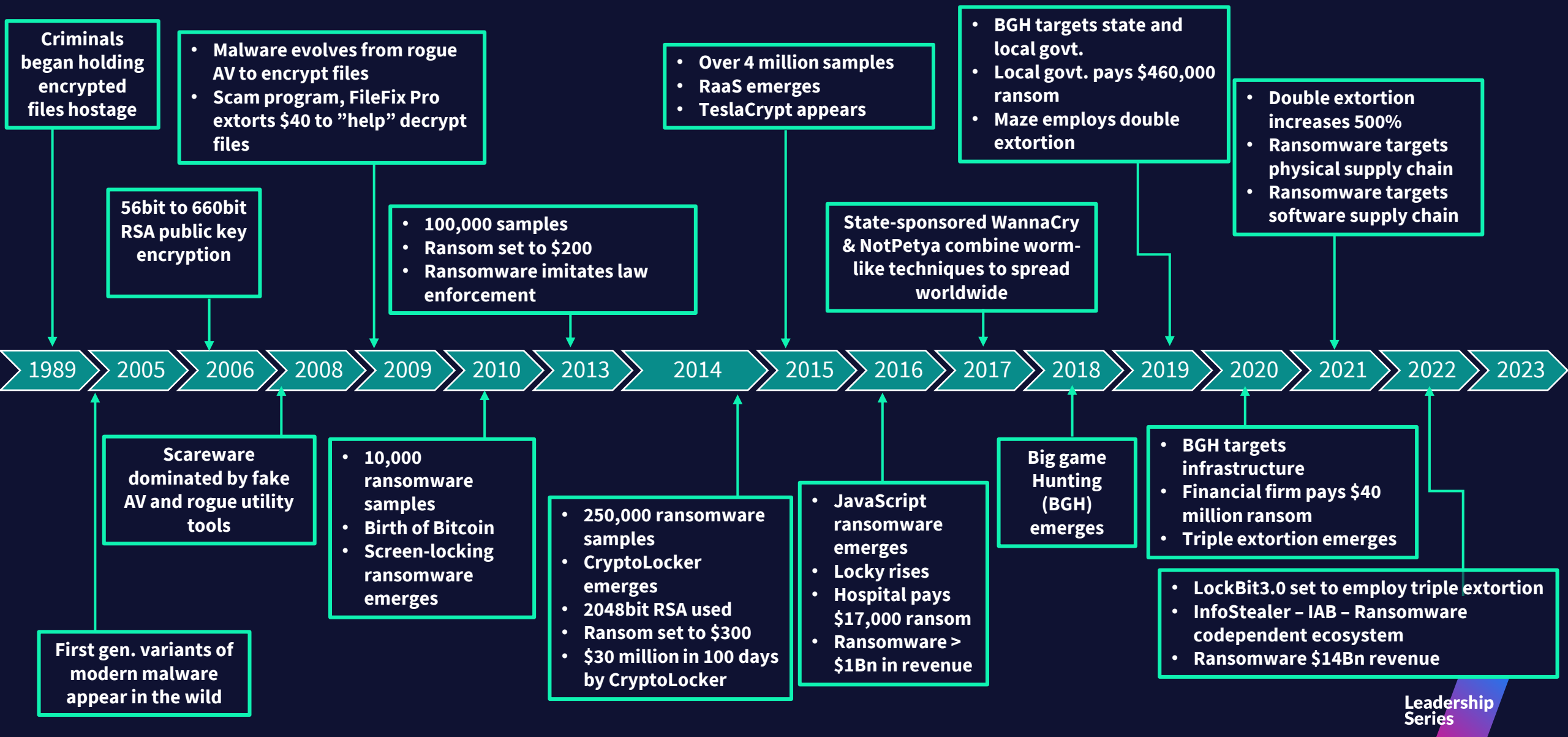
Iran

- APT35, Charming Kitten, Nemesis Kitten, Phosphorus, TunnelVision (2022 – most recently moonlighting for financial gain)
- APT34, Agrius, MuddyWater, N3tw0rm (2017)

North Korea

- Lazarus Group (2017 – WannaCry)
- H0lyGh0st (2021)

How ransomware developed



Evolution of extortion

Maximising revenue remains the core function of ransomware operations:

Single Extortion

- Encrypt data, pay for decryption key

Double Extortion

- Exfiltrate data
- Encrypt data on network, pay for decryption key
- Publish (or sell) data if ransom is not paid

Ransomware Revenue (Chainalysis)

- 2021: $768M
- 2022: $457M
- 2023: $449.1M to June 23
- 2023 projected: $898.6M
- *Based on Bitcoin wallet analysis, the true figure will be higher

Triple Extortion

- Exfiltrate data
- Encrypt data on network, pay for decryption key
- Publish (or sell) data if ransom is not paid
- Approach customers/clients of the victim and demand money for not leaking (sensitive data)

Ransom demands and payments

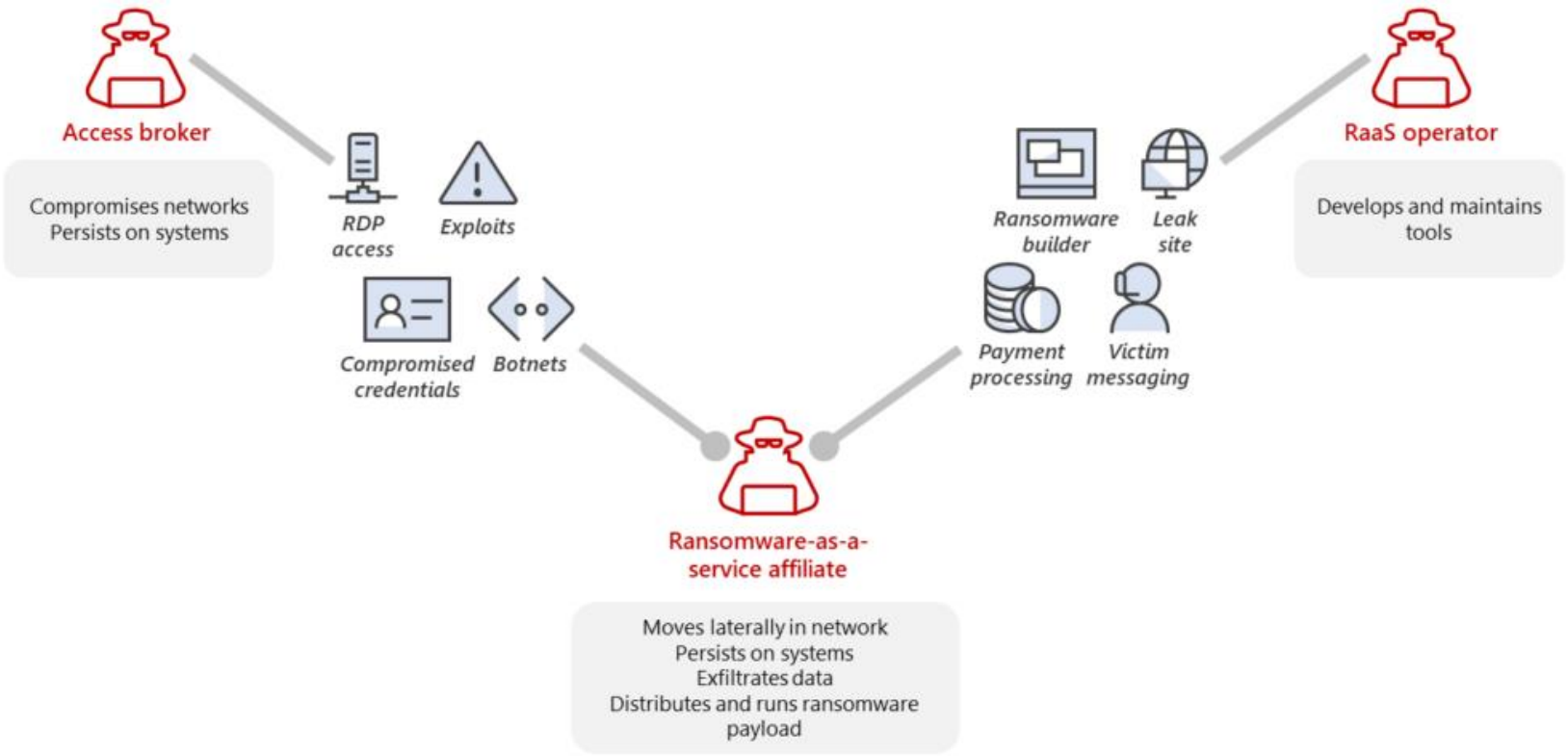
Estimated ransom vs revenue

- Difficult to track as they often occur on private channels
- Conti may have received $200M+ between 2017 and 2021
- Average ransom estimated at 0.16% of annual revenue
- Range: 0.02 – 0.37%
- Other factors include prominence, type of data compromised

Victim	Ransomware	Estimated Annual Revenue	Payments and Requested Ransoms	Percent of Ransom Demand Compared to Annual Revenue
Acer	REvil	$277 billion	$50 million	0.018
Brenntag	DarkSide	$13.4 billion	$7.5 million	0.056
CNA Financial Corp	Phoenix CryptoLocker	$10.8 billion	$40 million	0.37
Colonial Pipeline Company	DarkSide	$1.32 billion	$4.4 million	0.33
JBS	REvil	$53 billion	$11 million	0.02

Source: Recorded Future

Ransomware-as-a-service



Source: Microsoft

Revenue models:

- Monthly subscription for a flat fee
- Affiliate program: Subscription + % of profits
- One-time license fee, no profit sharing
- Pure profit sharing

Leadership Series

Initial access brokers

Facilitating ransomware operations:

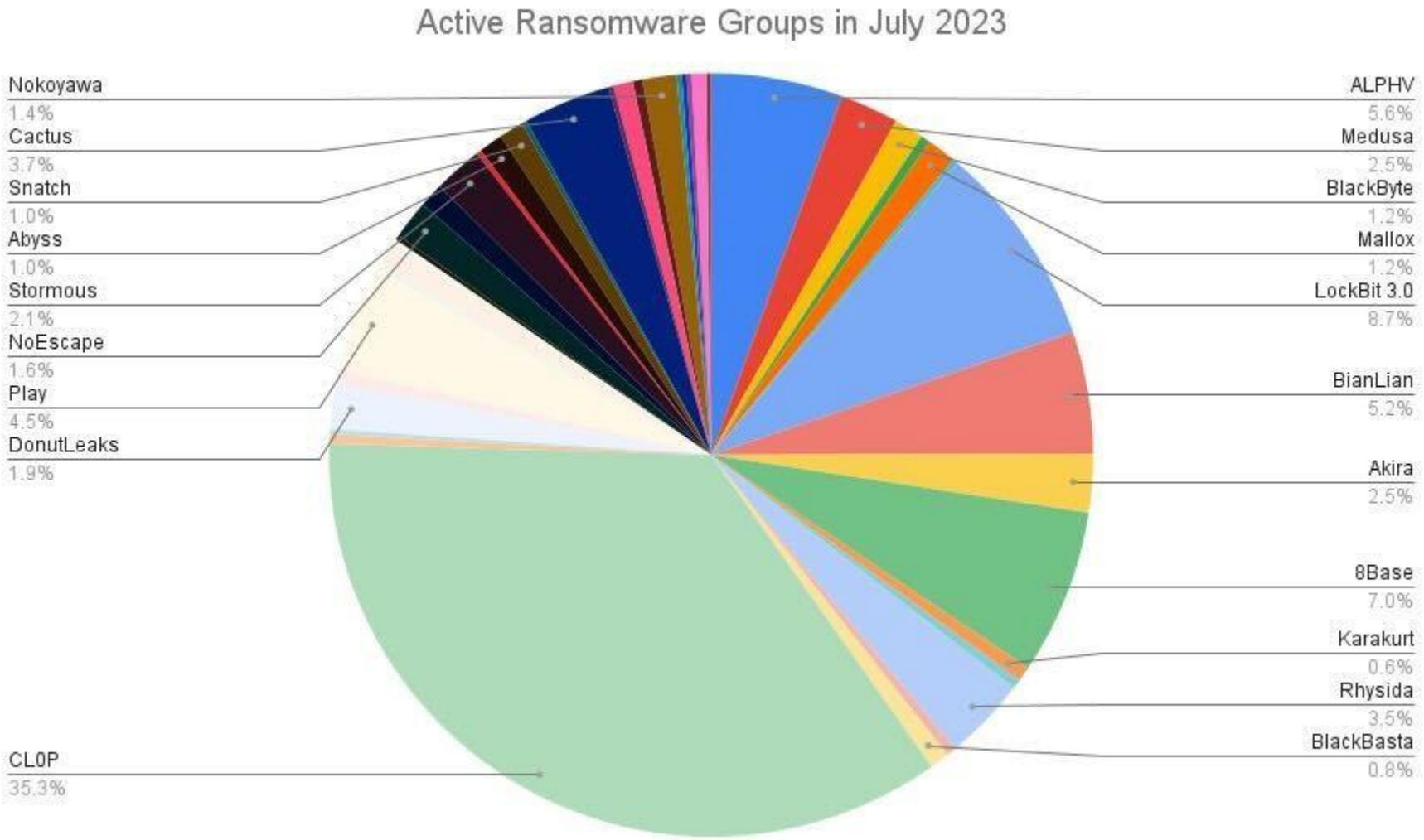
- Specialists who obtain and then sell access to ransomware operators
- Not always very technical – can be based on old exploits, misconfiguration or stolen credentials
- Can be very technical – such as quick deployment in response to zero days
- Access may be time-bound, particularly if based on a vulnerability for which a patch exists
- Fees between $1k and $10k to access a corporate network
- **Types of data:**
  - AD Credentials
  - Panels (control & interfaces)
  - Web Shells
  - RDP
  - VPN
  - Virtual Machine Access
  - Remote Monitoring & Management (RMM)

Ransomware in 2023

2

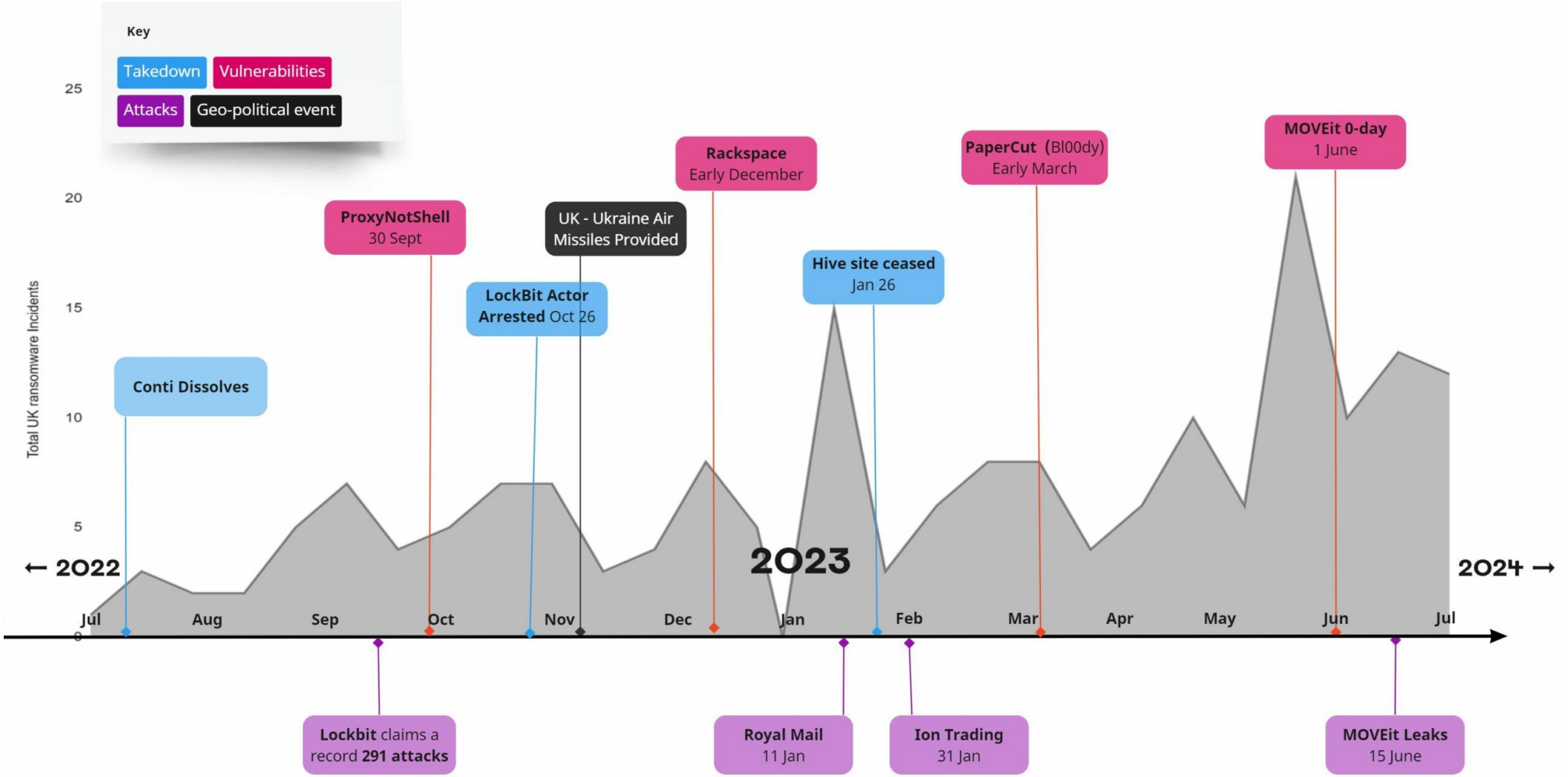
Leadership Series

Active ransomware groups



Leadership Series

UK ransomware activity July 2022 – July 2023



Leadership Series

Some key statements

- UK is second most targeted country (after the United States)
- Attacker-reported attacks in the UK have risen by 87% compared to the same period in 2022 (JumpSec)
- Dwell time for IAB: weeks to months
- Dwell time for ransomware operators: 4 – 11 days (Median)
- Average ransom: $1.5M, cost to business $4.5M (Sophos)
- Paying ransoms is more common in industries where downtime is unacceptable, such as manufacturing
- 65% who paid did not recover all data (Fortinet)
- 41% who paid did not receive as much from their insurer to cover the incident as expected, or in some cases received nothing at all due to an exception (Fortinet)
- Payment of ransoms to certain groups would breach sanctions

Observed TTPs

Key actions observed across threat actors:

- Targeting back-ups for encryption
- Encrypting incident response plans
- Targeting third parties (MSPs/Vendors etc.) to increase potential targets
- Threaten DDoS and media exposure to encourage ransom payment
- Sensitive data – threat of release to both the victim and their customers/users
- Cyber-knife fighting with admins when discovered

Implementing resilience

3

Leadership Series

Resilience Vs. Redundancy

- Resilience: *the capacity to recover quickly from difficulties; toughness*
- Redundancy: *the inclusion of extra components which are not strictly necessary to functioning, in case of failure in other components*
- Resilience may include elements of redundancy
- Should be modelled against threat scenarios (most likely and most dangerous)
- Risk-based decisions should be documented
- Incident lifecycle must still be followed, even when invoking DR plans
  - Don’t recover before you know *how* and *when* they got in
  - Restoring from compromised back-ups is a key gotcha

High-level guidance

Understand your business, network and third-parties

Critical to success – what is important, where is it, how to protect it, how to recover it.

What are your third-party dependencies?

Plan for Compromise

Plan for when, and not if.

Integrate IR plan with BCDR and Crisis Management Plans

Not just a cyber problem (or an insurance one)

Implement Controls

Measure existing controls, fix the gaps

Not all controls are technical

Review what insurance will cover

Exercise the plan(s)

Test the plan! (Don’t wait for an incident)

Honestly review performance – adjust the plan if required

Accept it won’t be perfect the first time around

Key issues

1

Roles and responsibilities

Key stakeholders not aware of their responsibilities, exacerbating incident through either inaction, or poor action

2

Incident response plans

Plans are not in place, not complete or not practiced

3

False view of security posture

Great dashboard = great security

Poor practices, poor training, slow/ineffective patching

Lack of verification of what should be done v what has been done

Leadership Series

User activity

Issue

User opening malicious files or clicking on malicious links

Users are the weakest link in any organisation making them an ideal target

Phishing attempts are one of the easiest and low-effort ways to deliver malicious content.

A little research on the organisation and key individuals can result in some very realistic phishing emails.

Remediation action

Limit the impact of user subversion

User awareness training

Implementation of web filtering

Implementation of email filtering

Understand risks to your business

Issue

Insufficient security controls protecting critical and sensitive data

Lack of knowledge of where the 'Crown Jewels' data/assets are located

Difficulty implementing means that it is difficult to ensure the right controls are in place

Lack of visibility/understanding of assets on the network perimeter and internal network

Remediation action

Know your business, know your network

Business impact assessment

Identify where critical and sensitive data is located

Identify critical assets – prioritise support

Assess the impact of loss of assets or data

Assess controls implement control

Implementation of email filtering

Asset inventory – determine actual network assets, including shadow IT

Subscribing to threat intelligence services

Credential hygiene

Issue

Stolen and/or unprotected credentials and identities

Credential and identity theft/abuse is more common than malware as the method of entry to a network or system

Used in nearly all successful ransomware attacks

Access to privileged and/or administrator-level accounts

Remediation action

Authenticate identities

Implement MFA on all accounts

Prioritise sensitive and admin accounts

Implement MFA on all devices (hybrid environments)

Password policy and enforcement

Role separation

Control the number of privileged accounts

Implement joiners/leavers/movers processes

Security products

Issue

Missing or misconfigured security products

Seen in nearly all successful operations

Key products are either missing or misconfigured

Enabled attackers operate without detection, tamper or otherwise disable protective

Alert fatigue/alerts are ignored or not understood

Remediation action

Remediate blind spots

Verify perimeter security posture

Verify the actual configuration of security systems and products

Include active directory configuration as a security tool

Patch and check patches have been applied correctly

Regular review and testing of security products

24/7 monitoring and response

Applications

Issue

Missing or misconfigured applications

Poor patching and/or config can lead to an adversary exploiting functionality to facilitate ransomware operations

Exploitation of poor permissions control

Exploitation of legacy/obsolete applications

Remediation action

Harden assets

Patch, harden and verify internet-facing applications

Review permissions and access control

Implement a robust patching regime across the enterprise and verify it is effective

Patching

Issue

Slow patching

Automated scanning for vulnerabilities, often within 24-48 hours of a critical vulnerability being announced

Viable exploits can be available within hours/days

Many organisations do not patch or do not verify patching is successful

Remediation action

Robust patching regime

Patch, harden, and verify internet-facing assets

Patch, harden, and verify core and critical systems

Asset inventory – determine actual network assets, including shadow IT

Identify critical assets – prioritise support

Identify legacy/obsolete or otherwise difficult-to-maintain systems and implement a management process

Set and measure patching objectives

Back-up and archives

Issue

Encryption of back-ups to increase the potential for a ransom payment

Internal reconnaissance identifies accessible back-ups

Back-ups can be encrypted first so that the victim is unable to conduct a restore

Remediation action

Back-up AND archive

Review back-up policy, procedures, locations and mechanisms – do they work, are they secure?

Immutable back-ups

Implement off-line archives where possible

Segmentation – restrict adversaries from being able to traverse across the whole network

Testing – do they work and how long to restore?

Testing – can an adversary get to them?

Government services

The Record from Recorded Future News

British intelligence is tipping off ransomware targets to disrupt attacks

By The Record | Published Aug 21, 2023

Article Entities Sources

On average, every 72 hours for the past three months, cyber experts inside one of the **United Kingdom**'s security and intelligence services have detected the beginnings of a new **ransomware** attack against a British organization and then tipped off the target in a bid to prevent the attack from being executed.

https://app.recordedfuture.com/portal/analyst-note/shared/true/doc:sYGOX5

If law enforcement or NCSC ever reach out invoke your IR plan

Welcome to Early Warning

The NCSC provides a free service to organisations to inform them of threats against their networks.

What is this service?

The NCSC's Early Warning service processes a number of UK-focused threat intelligence feeds from trusted public, commercial and closed sources, which includes several privileged feeds not available elsewhere.

By providing details of the assets your organisation owns, Early Warning will deliver feeds of the following types of threat information:

- **Incident Notifications** - Activity that suggests an active compromise of your system.
  Example: Your IP address has been involved in a DDOS attack.
- **Network Abuse Events** - Indicators that your assets have been associated with malicious activity.
  Example: A client on your network is a part of a Botnet.
- **Vulnerability Alerts** - Indications of vulnerable services running on your assets.
  Example: You have a vulnerable port open.

Early Warning complements your existing threat intelligence products, and should not be used in isolation.

Questions?

4

Leadership Series

LRQA NETTITUDE

Thank you

Leadership Series