Ransomware 2.0: Declining Giants, Emerging Threats, and Evolving Ecosystems

EQST of SK Shieldus

Experts, Qualified Security Team

About Me

Hyuna Lee

Threat Intelligence Researcher @EQST of SK Shieldus

Main Activity

Ransomware Research

Specialize

Tracking Attacker’s Infrastructure, Malware Hunting, Darkweb Monitoring

Others

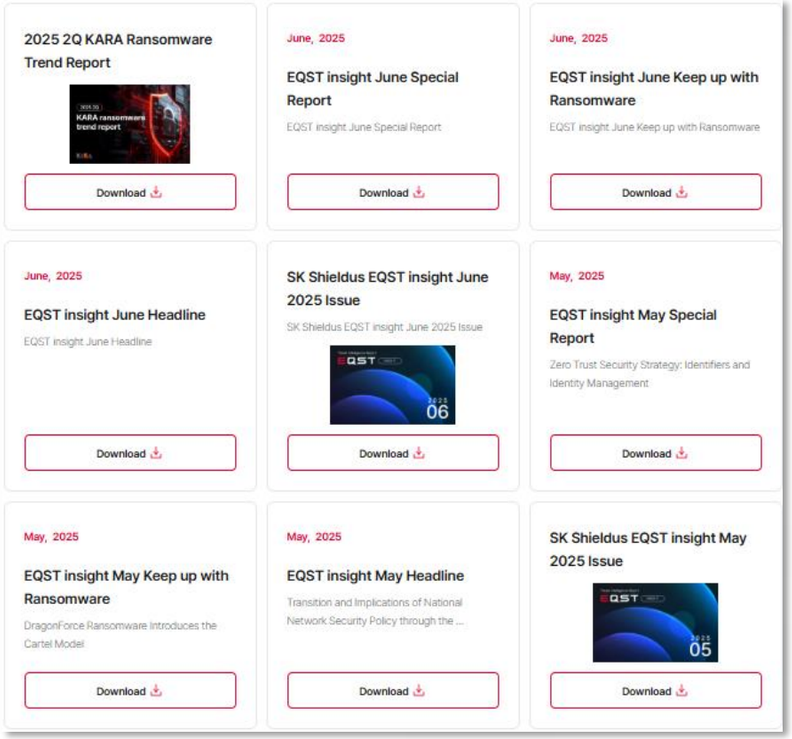
CTF Player

EQST
Experts, Qualified Security Team

About EQST

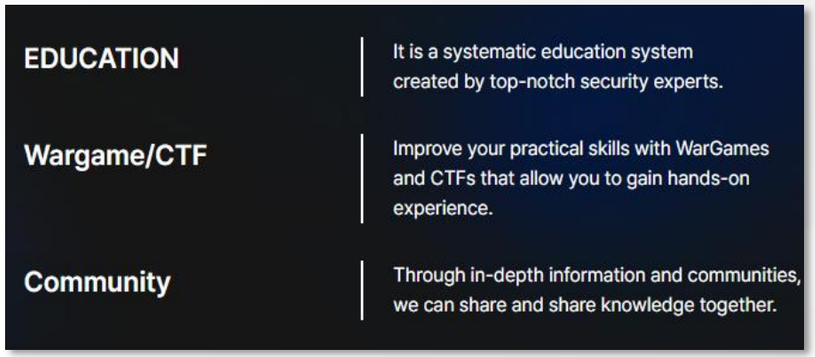
Stands for “Experts, Qualified Security Team”, we are the cybersecurity team of SK Shieldus.
We conduct research in various areas, including Web, Cloud, Ransomware, AI and more.

Research

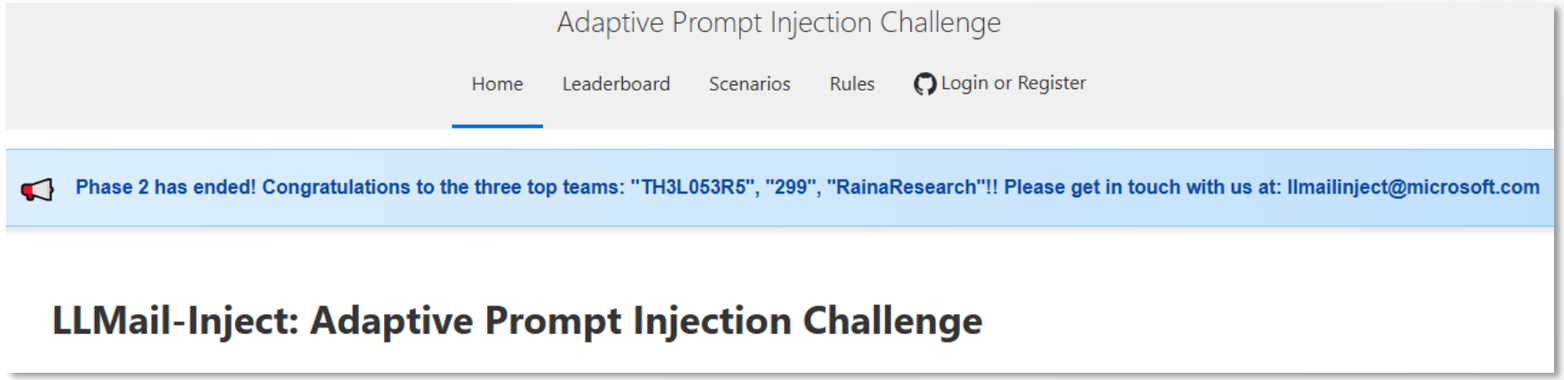


Conference

Education



CTF



EQST
Experts, Qualified Security Team

Outline

Session 1: The Changing Ransomware Landscape

Session 2: Unveiling the Actor's Arsenal

Session 3: Mitigation Strategies from the Front Lines

Conclusion

EQST
Experts, Qualified Security Team

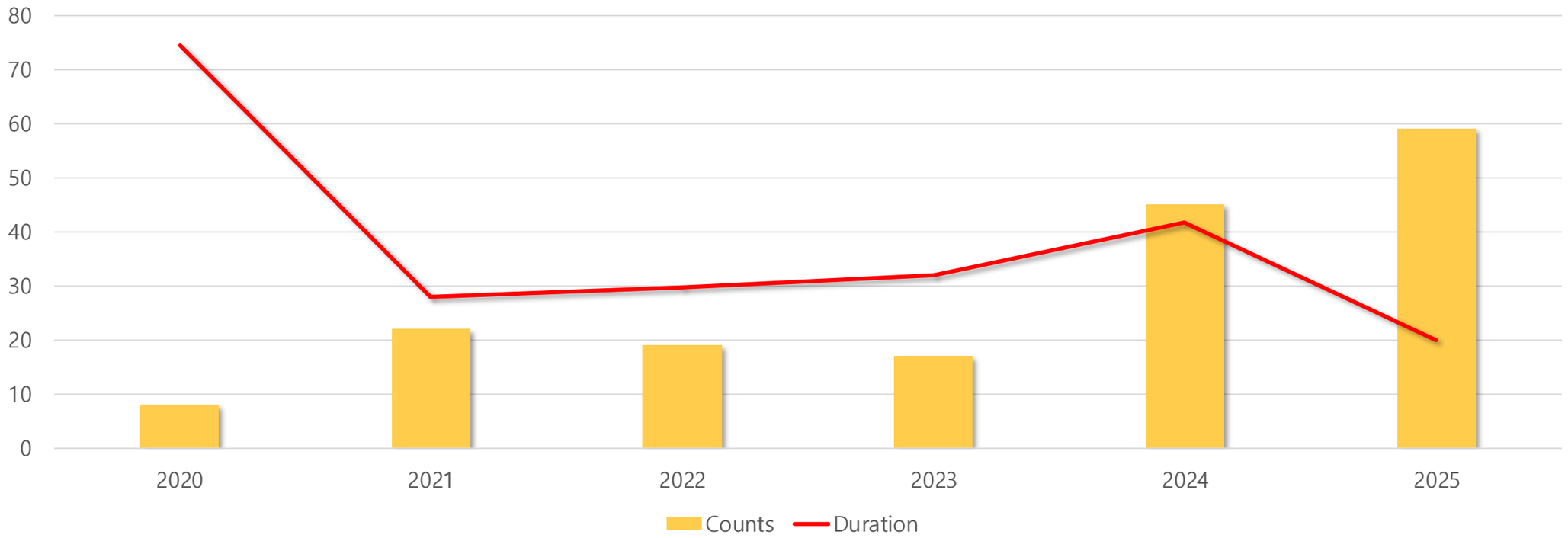
SESSION 01

The Changing Ransomware Landscape

01 The Fall of Major Groups and the Rise of Emerging Actors

More ransomware groups are vanishing within 12 months of appearing, and their life-cycle are getting shorter.

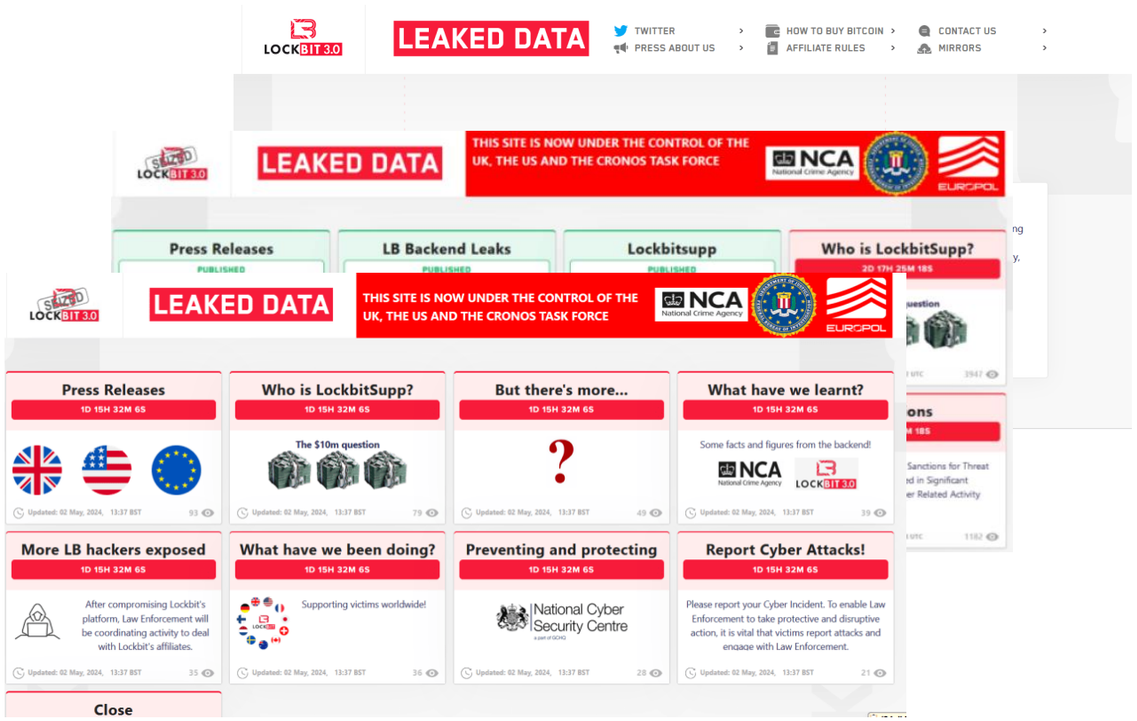
Status of Ransomware groups being destroyed



01 The Fall of Major Groups and the Rise of Emerging Actors

As ransomware damages continue to rise each year, law enforcement agencies are intensifying their efforts — seizing infrastructure and arresting key operators through various operations.

Operation Cronos



Operation Endgame

01 The Fall of Major Groups and the Rise of Emerging Actors

As ransomware damages continue to rise each year, law enforcement agencies are intensifying their efforts — seizing infrastructure and arresting key operators through various operations.

Infrastructure Seized

Group	Abstract	Period
8Base	Seizure of negotiation and leak sites, takedown of 27 servers, arrests and device confiscations	February 2025, Germany, Thailand, etc.
BlackSuit	Seizure of servers, domains, and digital assets (e.g., cryptocurrency), complete dismantling of infrastructure	August 2025, International Cooperation Led by the US
Hive	Seizure of servers and dark web infrastructure, FBI infiltration, recovery and distribution of decryption keys	January 2023, US and Europe Focused
Vanir	Seizure of dark web leak sites and takeover of TOR servers	September 2024, Germany
Dispossessor	Seizure of servers (3 in the US, 3 in the UK, 18 in Germany) and 9 domains	August 2024, International Cooperation Led by the US

01 The Fall of Major Groups and the Rise of Emerging Actors

BlackCat(ALPHV) and Mogilevich shut down their operations through an exit scam, disappearing without paying affiliates their share of the criminal profits.

BlackCat/Mogilevich Exit Scam

Hi here it's the Mogilevich group,
unfortunately this link led you to an important announcement of our business instead of evidence of a breached database.
You may be wondering why all this, and now I'm going to explain everything you need.
In reality, we are not a Ransomware as a Service, but professional fraudsters.
None of the databases listed in our blog were as true as you might have discovered recently.
We took advantage of big names to gain visibility as quickly as possible, but not to fame and receive approval,
but to build meticulously our new trafficking of victims to scam.

We have sold exactly 8 panel accesses belonging to our private infrastructure, something that in itself has never existed.
Initially, the price was a deposit of one thousand dollars,
When victims paid, we decided to double the deposit, we manipulated the victims giving him the choice of receiving the money back,
or updating the deposit with an additional thousand dollars.
From here, about sixteen thousand dollars are taken from the victims.
Have you wondered why we were asking for screenshots of potential buyers' crypto wallets?
Our goal was to use this evidence of funds to sell alleged accounts Crypto stolen under other identities.
From here we were able to take about seven thousand dollars from the victims.

We used social engineering pretending to be big buyers to get Initial Access Brokers to send us evidence of their accesses,
such as photos and videos. We've used all of this to sell fake accesses and to build our own credibility from Ransomware as a Service.
From here, about eleven thousand dollars are taken.
The biggest coup was made today . As you know, we have published a well-known drone company as a target.
The price for the alleged one-terabyte database was one hundred thousand dollars.
We were immediately contacted by interested people, One of them was put at ease, as if he were the boss at the time,
we explained to them that the data of that company They were private prototype projects, blueprints,
and that unfortunately even a small leak of data in the sample could cause great damage.
We made him believe that we had other buyers who were pressing us and that they wanted the projects as soon as possible.

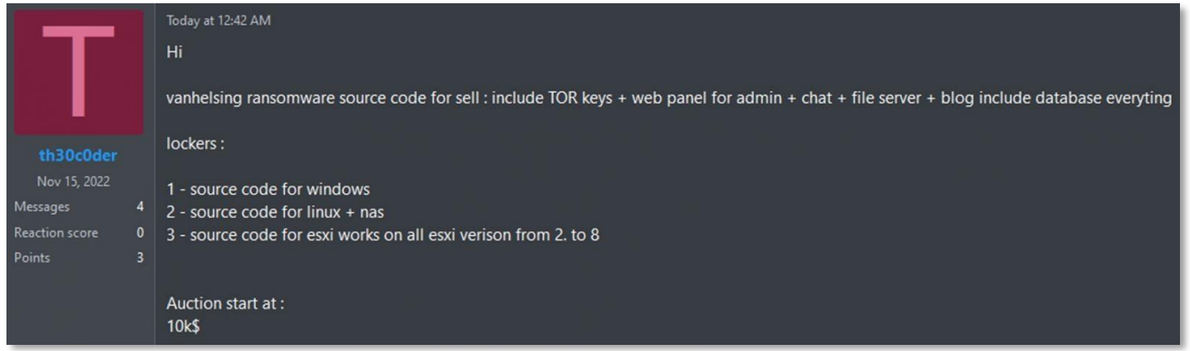
So seeing this, the victim did nothing but think that by doing so he would miss an opportunity.
After various techniques adopted to make ourselves credible, we came to terms by agreeing on a price of eighty-five thousand dollars.
Now the real question is? Why confess all this when we could just run away?
This was done to illustrate the process of our scam, We don't think of ourselves as hackers
but rather as criminal geniuses, if you can call us that. I think I've taught a lot of people,
especially Epic Games, a lesson that by creating ads and tweets has done nothing than advertise us by enlarging our fraudulent network.
My tox to confirm its me: E424A6FF3A035D58733AB6AC25353183691C380D9BA8DD0E4115923545 7BE574EFA8997FCD5

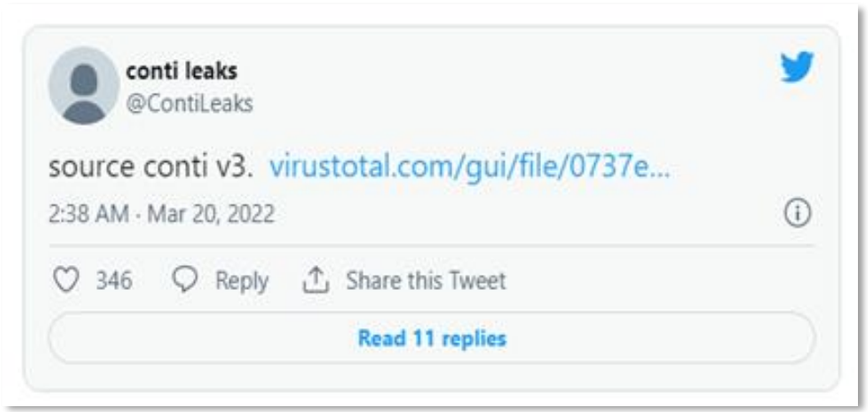
- Pongo

01 The Fall of Major Groups and the Rise of Emerging Actors

The leakage of source code or builders from major ransomware groups caused internal disruption and was also exploited in other attacks.

Builder/Source code leak

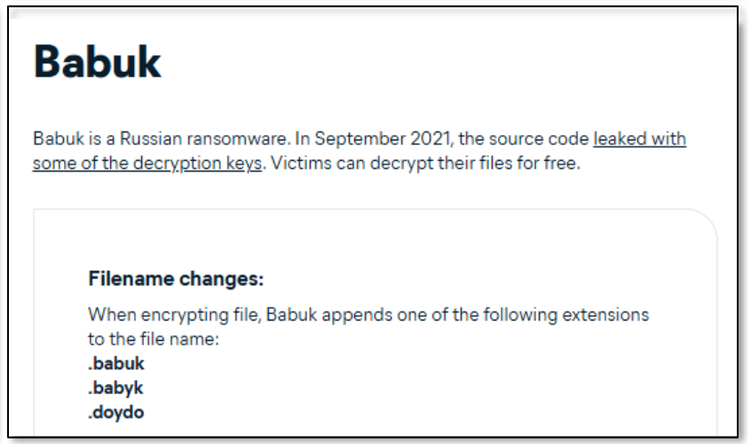




01 The Fall of Major Groups and the Rise of Emerging Actors

Ongoing research on developing decryption tools for major ransomware families such as Rhysida, BlackBasta, TargetCompany, and Babuk is helping to mitigate the impact on attacks.

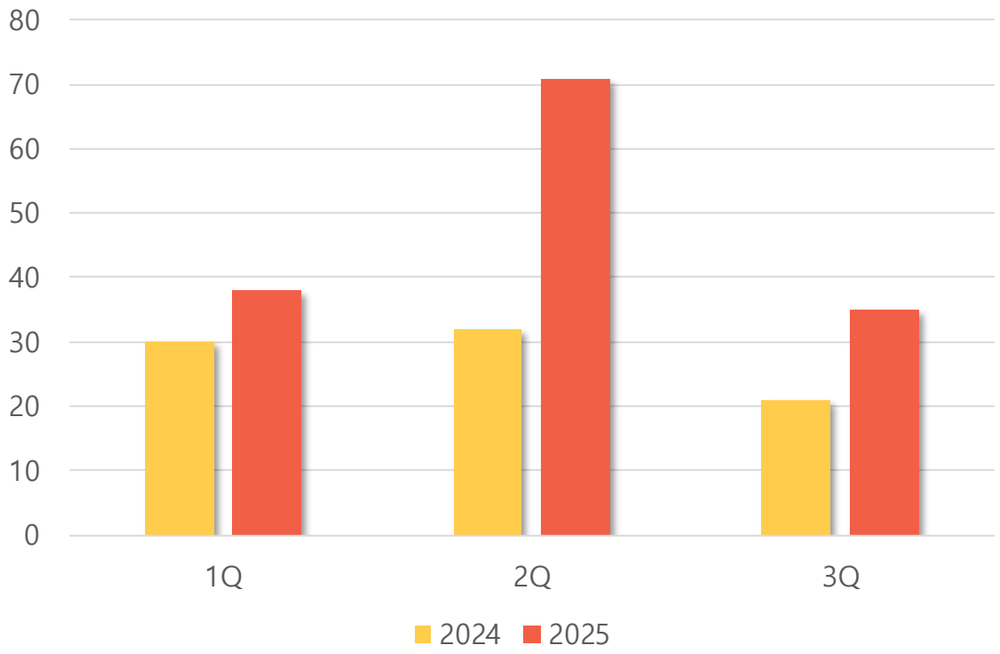
Development of Decryption Tools



01 The Fall of Major Groups and the Rise of Emerging Actors

The number of ransomware groups that emerged and disappeared within a single year has increased by about 1.7 times compared to last year.

The Rapid Rise of New Ransomware Groups



01 The Fall of Major Groups and the Rise of Emerging Actors

Major ransomware groups are reemerging under new branding, adapting their strategies in response to declining criminal profits and ongoing pressure from law enforcement agencies.

Strategic Shift Through Rebranding

Zeon
2022.02

- Single Extortion
- Python-based

Royal
2022.09

- Double Extortion
- Ceased operations after Dallas attack

BlackSuit
2023.05

- Evolution of Attack TTPs
- Operation Checkmate

Hive
2021.06

- Multi-extortion
- Go → Rust
- $100M ransom demand
- 2023.01 Seized

Hunters International
2023.10

- Inherited Hive's TTPs
- Over 200 attacks
- Shutdown of Activities and Release of Decryption Keys in Nov 2024

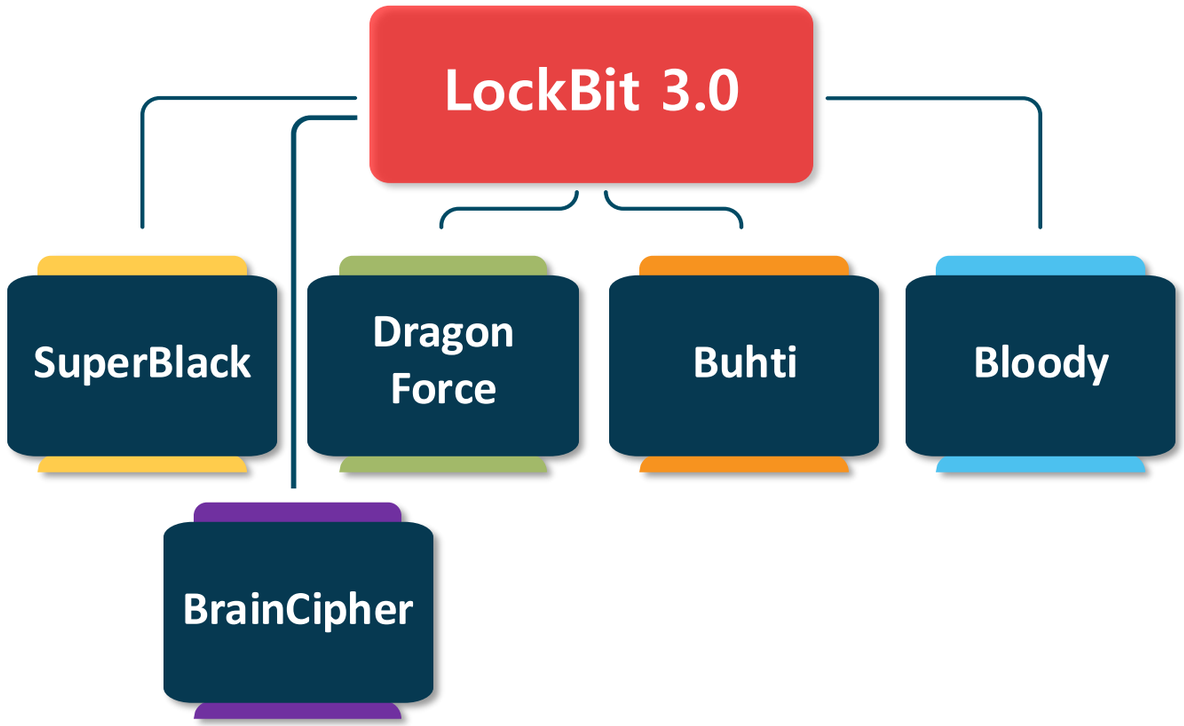
WorldLeaks
2025.05

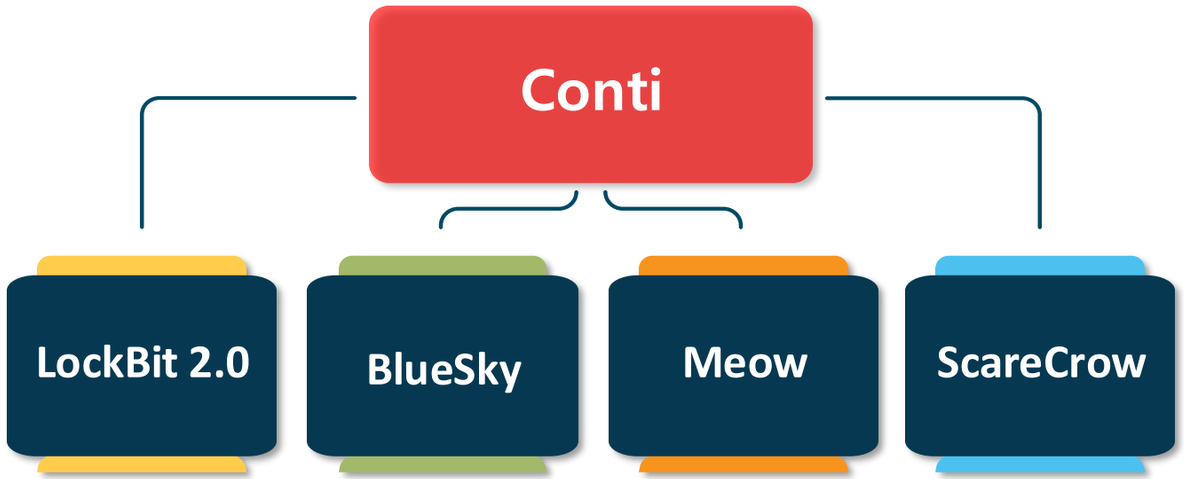
- Ceased Ransomware Operations and Pivoted to Data Brokering
- Despite declining ransomware market revenue, data-exfiltration revenue rose 41%

02 Attackers' Survival Strategies

Recently, ransomware groups have been leveraging leaked builders and source code to reduce operational resources, indicating their evolution from simple ransomware groups into a business-driven criminal ecosystem.

Operational Efficiency through the Use of Leaked or Publicly Available Tools

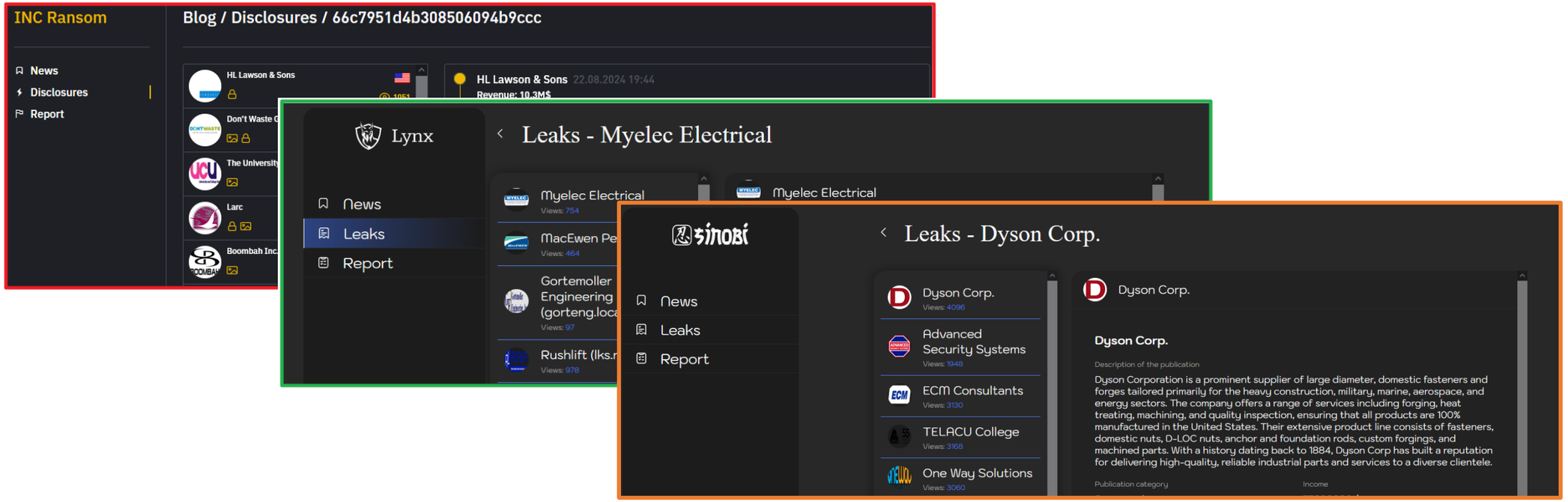




02 Attackers' Survival Strategies

Recently, ransomware groups have been leveraging leaked builders and source code to reduce operational resources, indicating their evolution from simple ransomware groups into a business-driven criminal ecosystem.

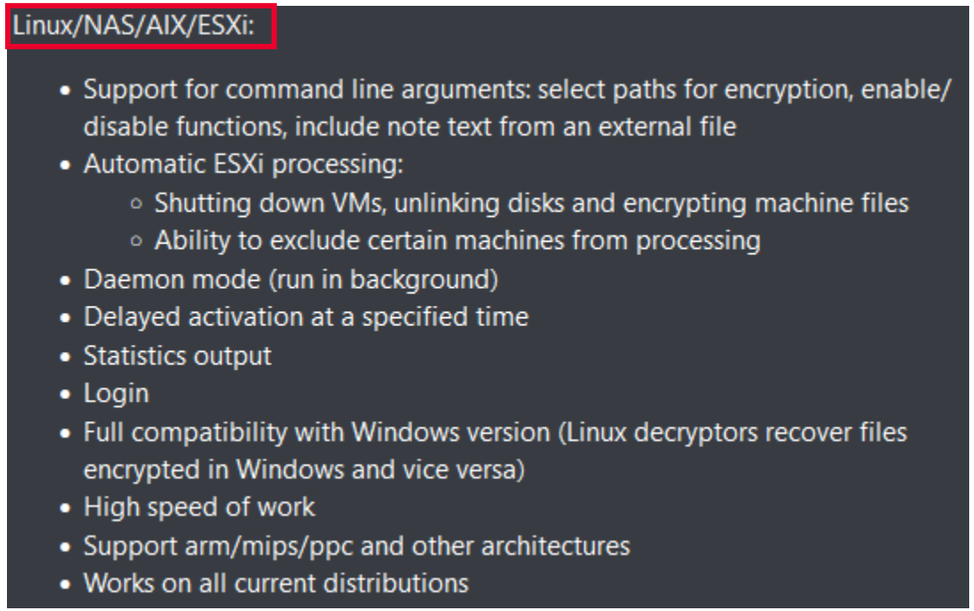
INC source code sold → Purchased by Lynx and Sinobi to develop their own ransomware



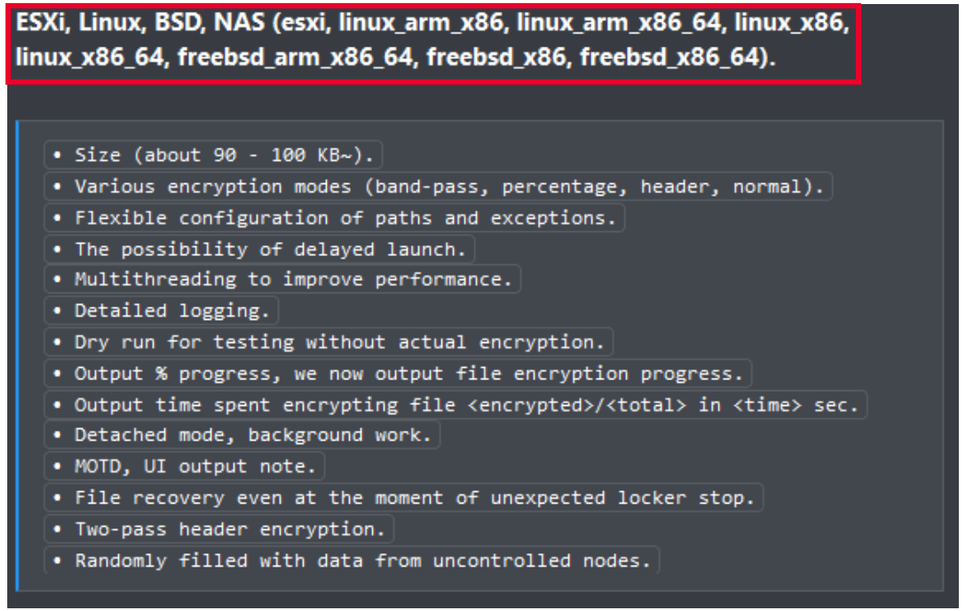
02 Attackers' Survival Strategies

Recent ransomware groups, facing declining criminal profits, are no longer targeting a single platform. Instead, they attack multiple platforms, threatening not only individuals but also critical infrastructure of businesses.

Expanding Targets Through Multi-Platform Attacks



Beast Ransomware

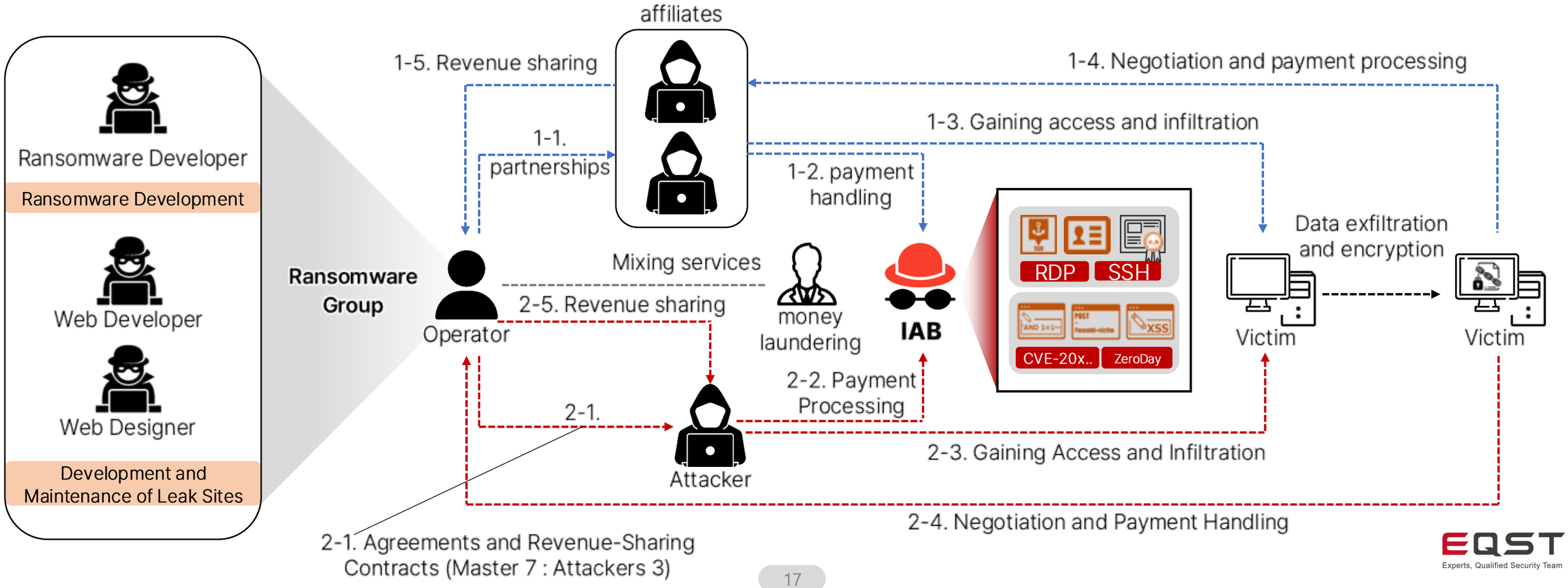


DragonForce Ransomware

02 Attackers' Survival Strategies

Many of the newly emerging ransomware groups are collaborating with IABs or adopting RaaS models, showing a trend toward specialization. This approach appears aimed at reducing operational burden while enabling more efficient and numerous attacks.

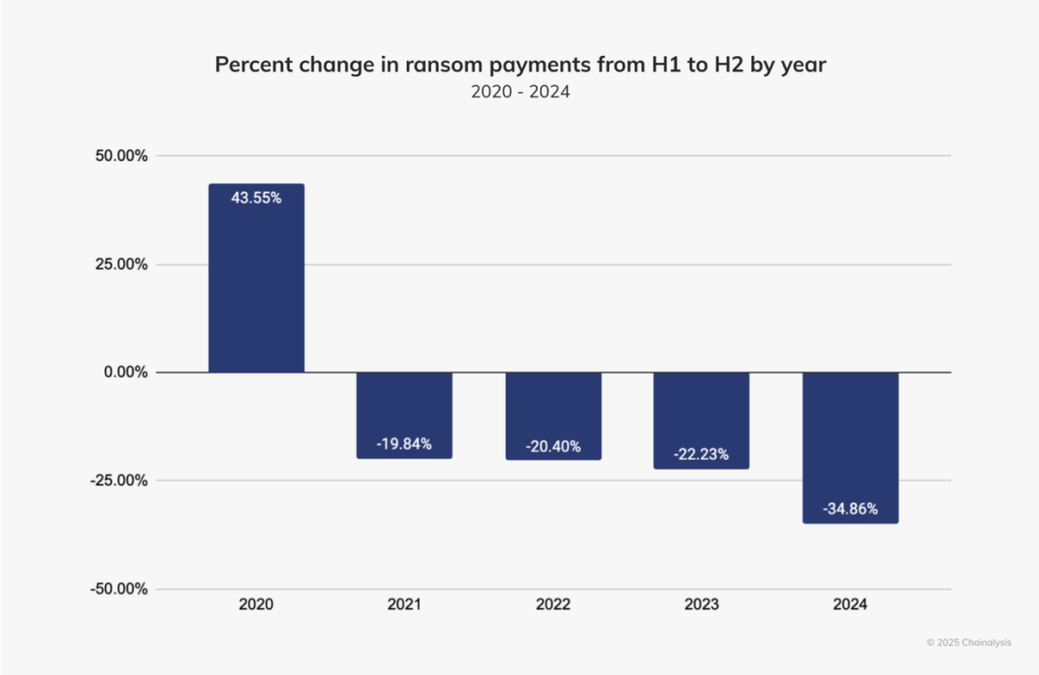
Operational Specialization Through RaaS Adoption and Collaboration with IABs

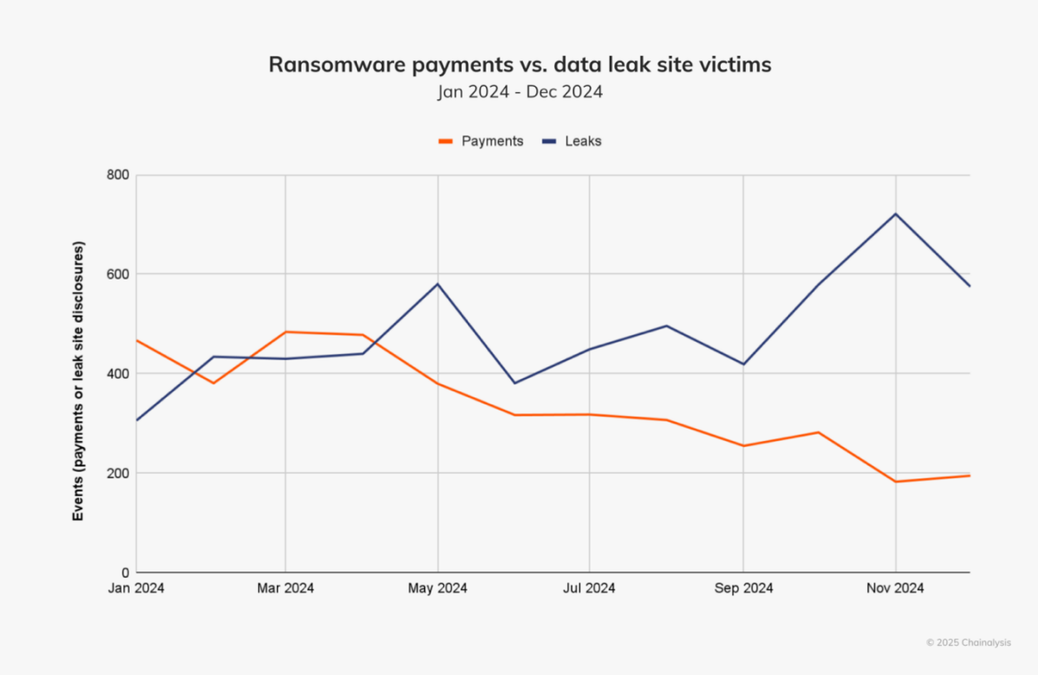


02 Attackers' Survival Strategies

While ransomware damages are increasing, the rate at which victims pay ransoms is declining. To adapt, attackers are changing their business models, not only encrypting data but also threatening to leak sensitive information on DLS platforms as part of a data exfiltration extortion strategy.

Changes in business models





Source: Chainalysis

02 Attackers' Survival Strategies

Although ransomware incidents are on the rise, the rate of ransom payments by victims is declining. To adapt, attackers are modifying their business models, employing strategies that not only encrypt data but also threaten to leak sensitive information on DLS platforms.

Changes in extortion methods

BianLian

'22~'23 Double Extortion

'23~'24
Decrease in Encryption, Increase in Data Exfiltration

Since '24
Pivoting to Data Extortion Model

Clop

'19 Double Extortion, RaaS

Since '21
Decrease in Encryption, Increase in Data Exfiltration

Large-scale attacks exploiting vulnerabilities

WorldLeaks

Hive, Hunters: Double Extortion

'24.11
Hunters shutdown of Operations

'25.01
Pivoting to Data Extortion Model

02 Attackers' Survival Strategies

As law enforcement investigations increasingly impact major ransomware groups, attackers are enhancing the anonymity of the infrastructure they use to evade tracking.

Changes in Infrastructure Operations to Evade Investigations

Reverse Proxy

Hiding real server Ips: Requests handled via proxies

Multi-layered proxies to hinder tracking: Placed in front of Clearnet

Easy server replacement: Backend swapped even if one is seized

CDN

Service provided via CDN edge servers: Users connect to the nearest server

Hiding real server IPs: Only CDN nodes are exposed

Traffic filtering: Protects against attacks and manages certificates

Bulletproof Host

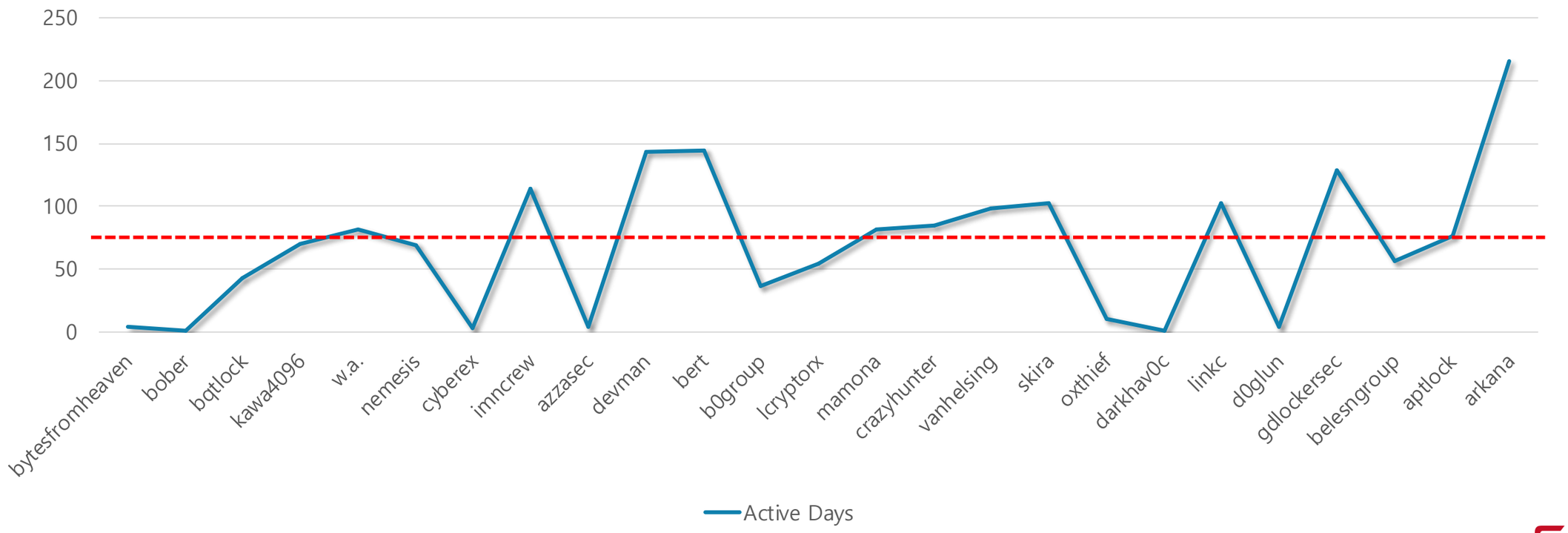
Legal enforcement is hinder: Crypto payments, anonymous sign-ups, limited cross-border cooperation

Operational model: origin Servers on BPH fronted by reverse proxy and CDN.

02 Attackers' Survival Strategies

While traditional ransomware groups operated over several years, newly emerging groups tend to conduct short-term campaigns and quickly cease operations to avoid law enforcement investigations and punishment.

Rapid Cessation of Operations



02 Attackers' Survival Strategies

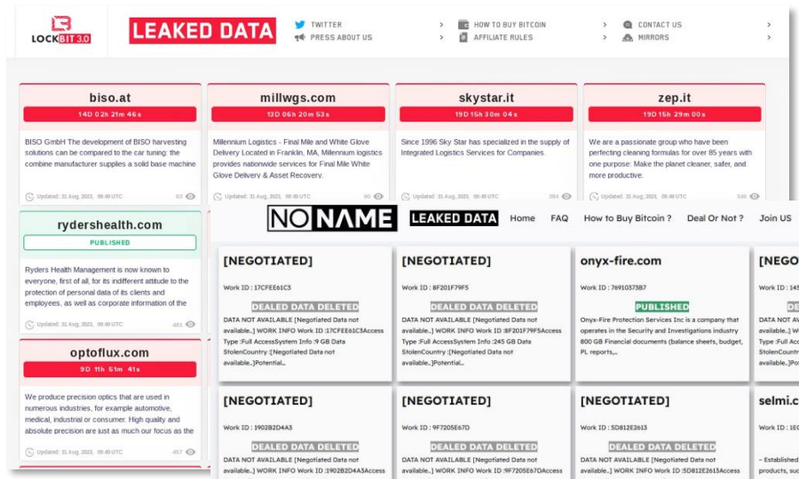
Newly emerging ransomware groups have been observed imitating the strategies of previously impactful major groups, aiming to minimize operational risks while maximizing profitability and recognition.

Imitating Notorious Groups

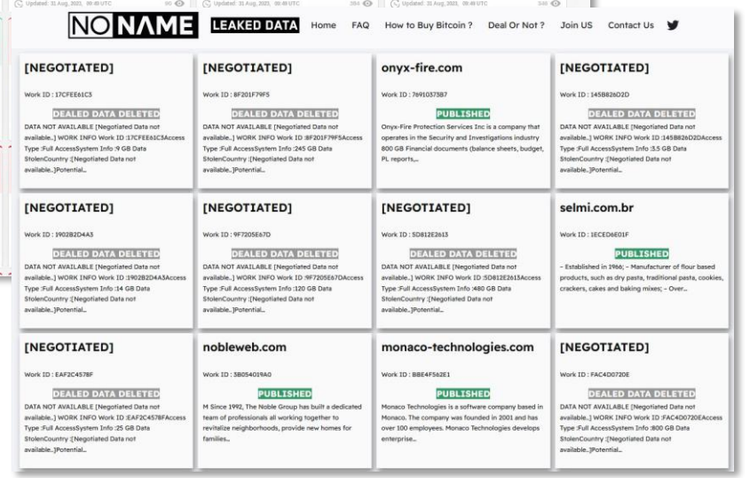
Akira

Kawa4096

Vanir



LockBit



NoName

02 Attackers' Survival Strategies

Recently, ransomware groups have been leveraging leaked builders and source code to reduce operational resources, indicating their evolution from simple ransomware groups into a business-driven criminal ecosystem.

In the past, large groups dominated the landscape, but today, leaner emerging groups are rapidly appearing and disappearing.

The cohesion of existing groups has weakened due to investigations, insider reports, and internal leaks, creating a gap that is being filled by new groups

New groups minimize operational resource consumption by imitating existing groups or leveraging leaked resources.

Increasing Trend of Data-Extortion-Only Groups, Focusing Solely on Data Theft Rather Than Encryption

SESSION 02

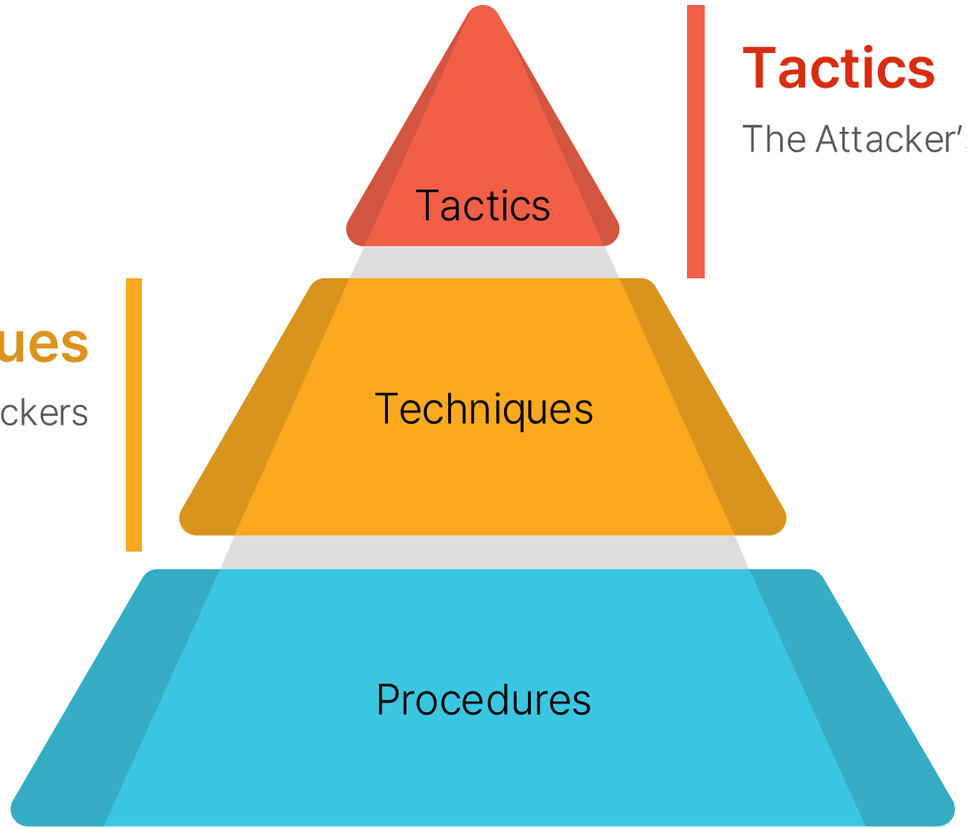
Unveiling the Actor’s Arsenal

01 Ransomware Attack Analysis Based on MITRE ATT&CK

MITRE ATT&CK is a framework that models adversary tactics and techniques, providing detection and mitigation methods.
It helps identify attacker strategies, build tailored defenses, and support attribution.

Mitigations & Detections

Recommended Countermeasures and Detection Methods for Each Technique



Tactics

The Attacker's Objective Behind the Action

Techniques

Methods Used by Attackers to Achieve Their Tactics

Procedures

Detailed Techniques to Achieve the Attack Method

01 Ransomware Attack Analysis Based on MITRE ATT&CK

Frequently employed ransomware tactics provide a means to depict the complete attack progression—from first compromise to the encryption of data.

Initial Access

Use of Stolen or Weak Credentials
System & Application Vulnerability Exploitation
Intrusion via IAB-Purchased Access

Execution

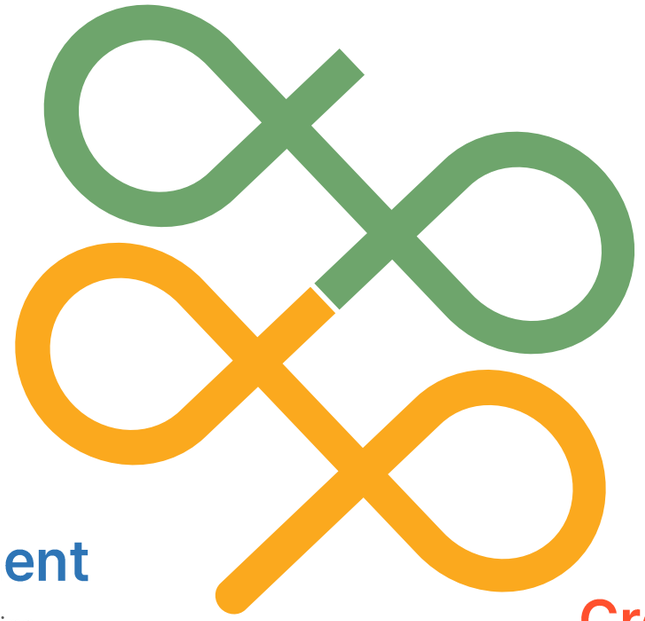
PowerShell, CMD, and WMI commandsScripts such as VBS, JS, and PythonUse of penetration-testing tools

Impact

Data encryption via ransomware
Disabling backup copies and recovery functionsService shutdown

Privilege Escalation

Access token theft via WinAPI and malware
Bypass via special privileges and UAC manipulation
Exploitation of driver and software vulnerabilities



Command and Control

Filtering bypass via common services
Indirect connections via proxies
File transfer using publicly available tools and commands

Defense Evasion

Encryption of configuration values
Use of crypters and packers
Use of tools to disable security solutions

Lateral Movement

Remote access service logins
Internal propagation via network shares and DCOM
RMM-based malware propagation

Credential Access

Use of LSASS dump tools
Information theft via infostealers
Use of penetration-testing tools

01 Ransomware Attack Analysis Based on MITRE ATT&CK

Recently, the initial infection methods of ransomware attacks have diversified. While phishing and pirated software downloads were once the main infection vectors, social engineering techniques such as ClickFix and malvertising are now common, along with widespread exploitation of vulnerable services.

Evolution of Distribution Methods

ClickFix

Disguised as software updates, victims are tricked into entering malicious command in File Explorer.

Malvertising

Placing malicious ads in search engines to trick users into downloading files

Phishing

Delivery of malicious attachments or links via email

Pirated Software

Installing ransomware disguised as crack files or keygens

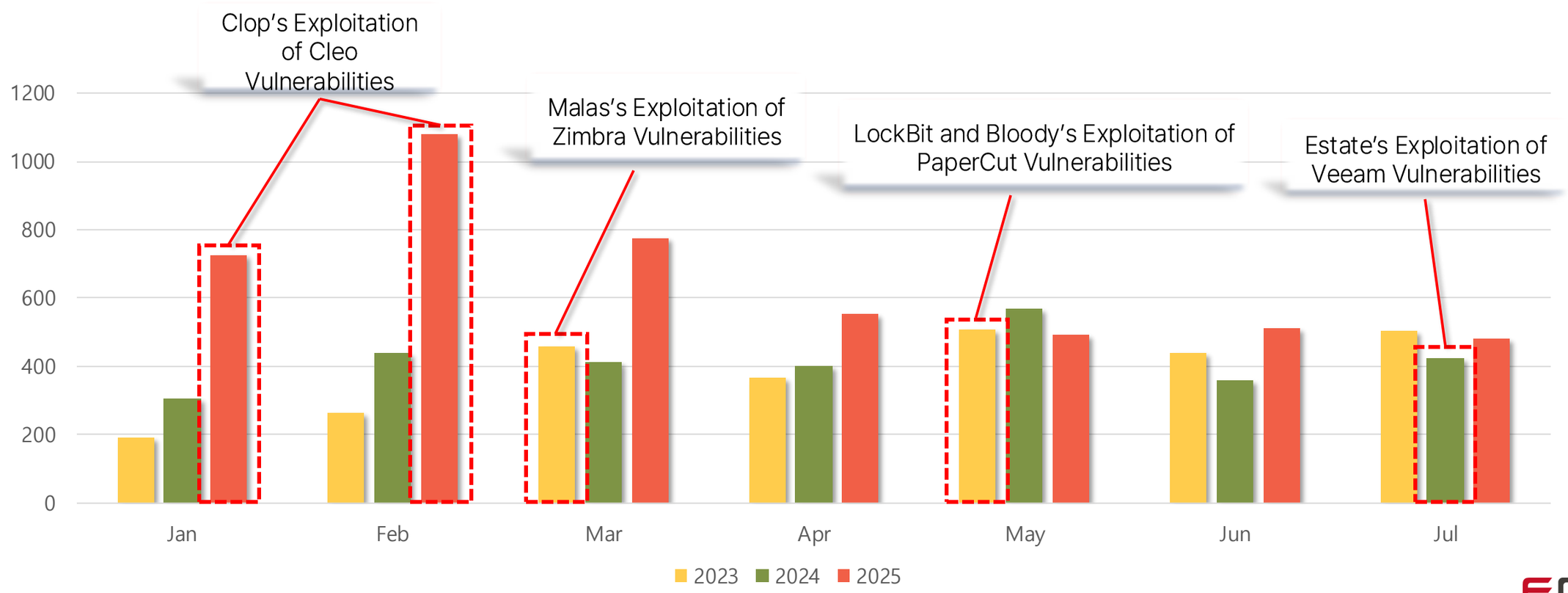
Vulnerable Service Attacks

insecurely managed Misconfigured externally exposed services such as VPN and RDP can be infiltrated through scanning.

01 Ransomware Attack Analysis Based on MITRE ATT&CK

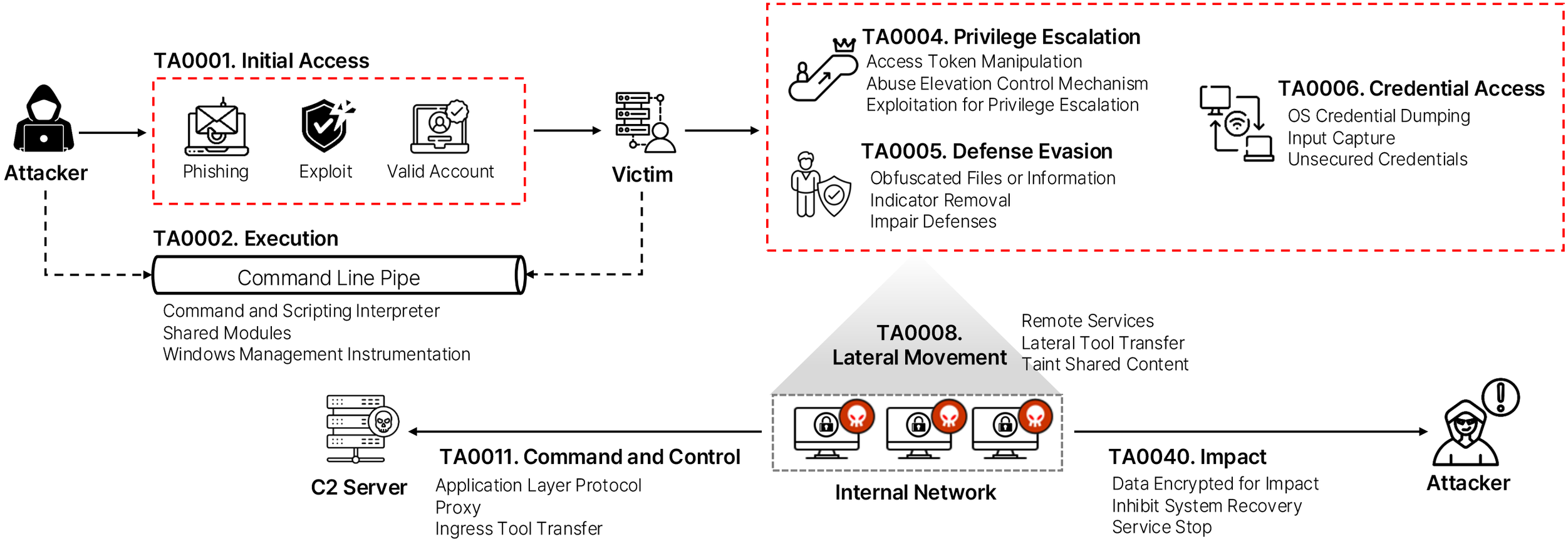
Among recent ransomware attacks, large-scale attacks exploiting vulnerabilities have emerged as a major threat. Attackers are increasingly conducting large-scale attack campaigns by exploiting vulnerabilities in software with a large global user base.

Large-Scale Attacks Exploiting Vulnerabilities



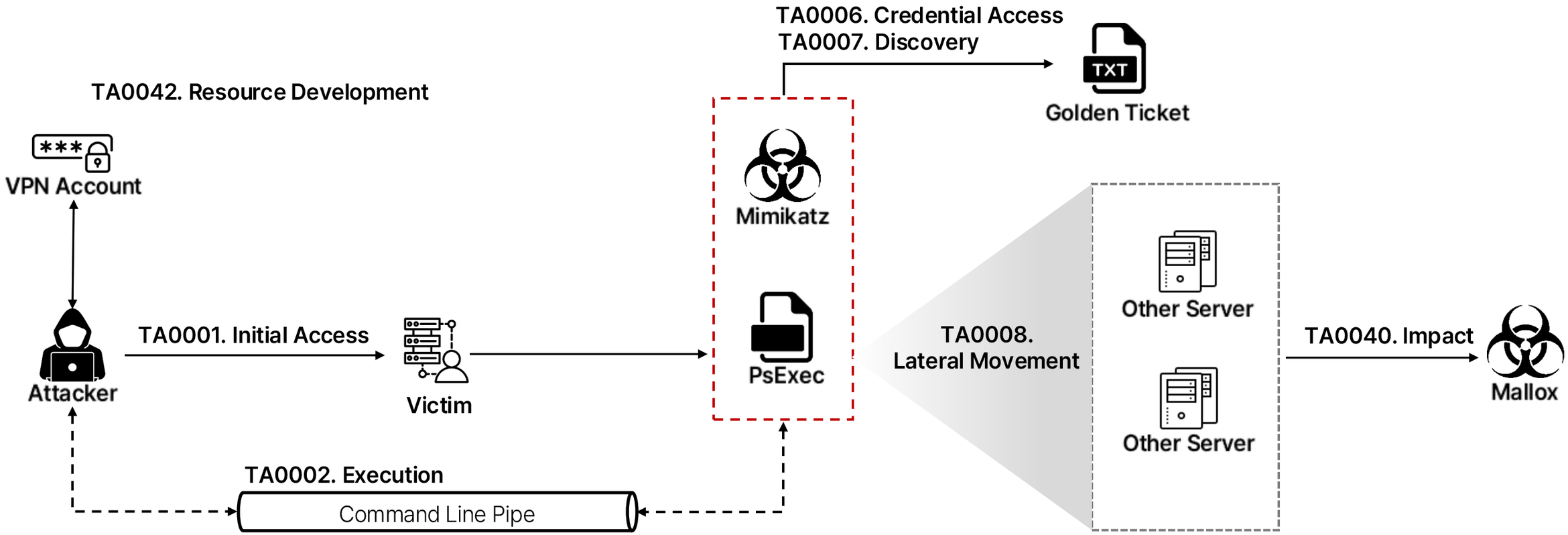
01 Ransomware Attack Analysis Based on MITRE ATT&CK

Ransomware attacks can be mapped with MITRE ATT&CK. By breaking down each stage of the attacker's strategy, we can design more effective responses and mitigation measures.



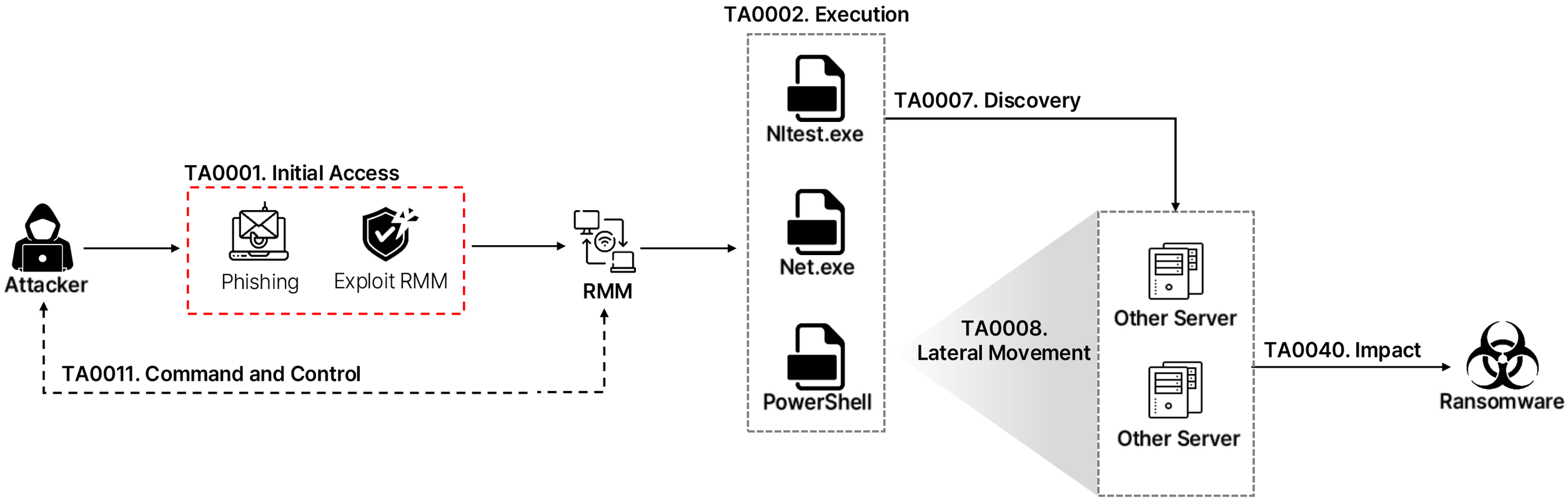
01 Ransomware Attack Analysis Based on MITRE ATT&CK

Scenario based on an actual ransomware incident case, showing tools and strategies at each stage.



01 Ransomware Attack Analysis Based on MITRE ATT&CK

Scenario based on an actual ransomware incident case, showing tools and strategies at each stage.



01 Ransomware Attack Analysis Based on MITRE ATT&CK

Ransomware groups often use legitimate tools in their attacks to avoid detection, as shown in actual ransomware incident case.

Recent Ransomware Strategies

LotL

[Medusa]
legitimate Windows tools and network scanners
PowerShell obfuscation and tunneling tools

[LockBit]
Use built-in Windows network commands
Remote ransomware execution via WMIC commands

[ViceSociety]
Use PowerShell scripts to bypass security
deploy ransomware via PsExec

BYOVD

[Qilin]
Use the IOCTL code of the driver for the laptop power saving function to execute shell code

[RansomHub]
Use EDRKillShifter to load vulnerable drivers

[Kasseika]
Vulnerable drivers can be exploited to shut down security solutions

RMM

[Hunters International]
Keep access to AnyDesk, ScreenConnect for data theft

[DragonForce]
Exploiting the vulnerability of SimpleHelp RMM to infiltrate MSPs and steal data

[Medusa]
After initial penetration with ScreenConnect, use PDQ Deploy for internal network scanning and malware distribution

SESSION 03

Mitigation Strategies from the Front Lines

01 Mitigation by key tactics

Ransomware prevention strategies can be built through mitigation across MITRE ATT&CK phases.

Tactic	Technique	Mitigation
Initial Access	Valid Accounts	[M1015] Active Directory Configuration, [M1026] Privileged Account Management
	Exploit Public-Facing Application	[M1050] Exploit Protection, [M1030] Network Segmentation
Execution	Command and Scripting Interpreter	[M1045] Code Signing, [M1049] Anti-Virus/Anti-Malware
	Windows Management Instrumentation	[M1040] Behavior Prevention on Endpoint, [M1038] Execution Prevention
Privilege Escalation	Abuse Elevation Control Mechanism	[M1047] Audit, [M1022] Restrict File and Directory Permissions
	Exploitation for Privilege Escalation	[M1048] Application Isolation and Sandboxing, [M1050] Exploit Protection
Credential Access	OS Credential Dumping	[M1043] Credential Access Protection, [M1025] Privileged Process Integrity
	Unsecured Credentials	[M1041] Encrypt Sensitive Information, [M1037] Filter Network Traffic
Lateral Movement	Remote Services	[M1035] Limit Access to Resource Over Network, [M1032] Multi-factor Authentication
	Lateral Tool Transfer	[M1031] Network Intrusion Prevention, [M1037] Filter Network Traffic
Exfiltration	Exfiltration Over Web Service	[M1057] Data Loss Prevention, [M1021] Restrict Web-Based Content
	Exfiltration Over Alternative Protocol	[M1030] Network Segmentation, [M1018] User Account Management
Impact	Data Encrypted for Impact	[M1040] Behavior Prevention on Endpoint, [M1053] Data Backup
	Inhibit System Recovery	[M1028] Operating System Configuration, [M1038] Execution Prevention

02 Reactive Response

In the event of a ransomware incident, a four-step process enables rapid and effective response.

Ransomware Response Procedure

Initial response

- Disconnect external storage
- Keep system powered
- isolate network
- Identify ransomware type
- Report to relevant agencies

Damage assessment

- Check system availability
- Check encryption scope
- Check network spread
- Check data exfiltration

Incident investigation

- Analyze attack surface
- Analyze system logs and artifacts
- Check for account compromise and privilege escalation
- Collaborate with relevant agencies
- Analyze attacker TTPs

Recovery & prevention

- Backup encrypted files
- Format or reinstall OS before restoring
- Use decryption tools if available
- Implement Zero Trust
- Conduct regular security training

02 Reactive Response

In many cases, victims negotiate with attackers to obtain decryption tools in exchange for money, but such negotiations remain a subject of social debate.

Negotiation with attackers

Ransomware is software used maliciously by cyber criminals to access victims' computer systems. Systems and data can be encrypted, or data stolen, until a ransom is paid. Ransomware is estimated to cost the UK economy millions of pounds each year, with recent high-profile ransomware attacks highlighting the severe operational, financial, and even life-threatening risks.

Public sector bodies and operators of critical national infrastructure, including the NHS, local councils and schools, would be banned from paying ransom demands to criminals under the measure, with nearly three quarters of consultation respondents showing support for the proposal.

In 2021, North Carolina became the first state to prohibit public ransomware payments, even going so far as to ban negotiations with cyber criminals. It was a groundbreaking move. Florida followed suit in 2022, but its legislation took a less stringent approach, covering a narrower range of entities and omitting some of the stricter provisions found in North Carolina's law.

'I don't see it happening': CISA chief dismisses ban on ransomware payments

OXFORD, United Kingdom — Jen Easterly, the director of the U.S. Cybersecurity and Infrastructure Security Agency, on Thursday poured cold water on suggestions the United States might bring in a ban on ransomware payments.

"I think within our system in the U.S. — just from a practical perspective — I don't see it happening," said Easterly at the Oxford Cyber Forum, an event run by the University of Oxford's Blavatnik School of Government and the European Cyber Conflict Research Initiative (ECCRI).

"Will it deter attacks? I think no. Should public sector organizations that use taxpayer money be paying criminals? I also think no," MacColl said.

"Anything that the government can do to force victims to be a little bit more deliberate about their decision-making around ransom payments would be positive. But ultimately, the goal should be making organizations more resilient in the first place," he said.

03 Proactive Defense

To prevent ransomware incident, it is important to implement security solutions and establish proper security policies.

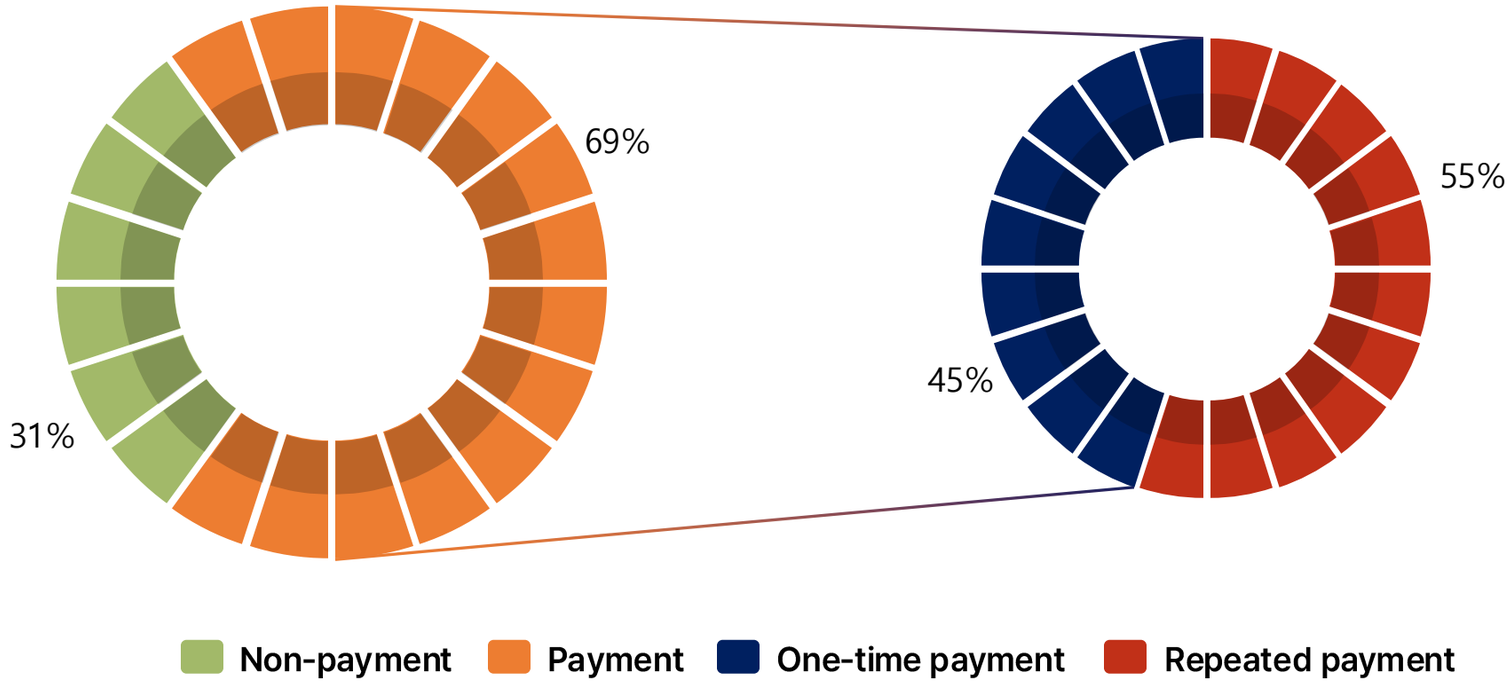
Preventive Measures

- Network segmentation, EDR/XDR/MDR and CTI to block early spread
- Stronger rules to detect attacker-abused tools (e.g., RMM)
- Zero Trust with least privilege and continuous verification
- Regular pentesting and checklist-based audits to minimize blind spots

03 Proactive Defense

Many victims obtain decryption tools through negotiations with attackers, but more than half suffer repeated attacks. Prevention remains the most effective response.

Need for proactive measures to prevent recurrence



03 Proactive Defense

To prevent ransomware incident, organization need to establish proactive security strategies. Active defense measures and strengthened organizational resilience can minimize the threat.

Resilience & Recovery

- Secure backups, cold backups, and use automated backup solutions
- Establishing Disaster Recovery and Business Continuity Plans (BCP)
- Rapid isolation → Damage-assessment → Secure recovery process
- Enhanced response through recovery training and simulations

04 Ransomware decryption

With active research on ransomware decryption, related organizations are distributing various decryption tools free of charge.

Decryption tool distribution platforms

SK shieldus

Avast

KISA
Korea Internet & Security Agency

kaspersky

EQST
Experts, Qualified Security Team

Conlusion

Conclusion

01 Conclusion

With the fall of major ransomware groups, new groups with diverse strategies are taking their place. This shift in the ransomware landscape highlights the need for thorough strategic analysis to develop tailored countermeasures for prevention and response.

Fall of major groups

- Stronger law enforcement
- Whistleblowing
- Insider leaks
- Development of decryption tools

Strategies of emerging groups

- Emergence of leaner groups
- Short-lived campaigns with rapid shutdown
- Data-theft–focused attack methods
- Highly segmented operational structures

Adaptive response

- As the landscape shifts, our response must evolve.
- Tailored countermeasures are needed through analysis of attackers' key strategies.
- Prevent damage through proactive measures and ensure rapid response by strengthening resilience.