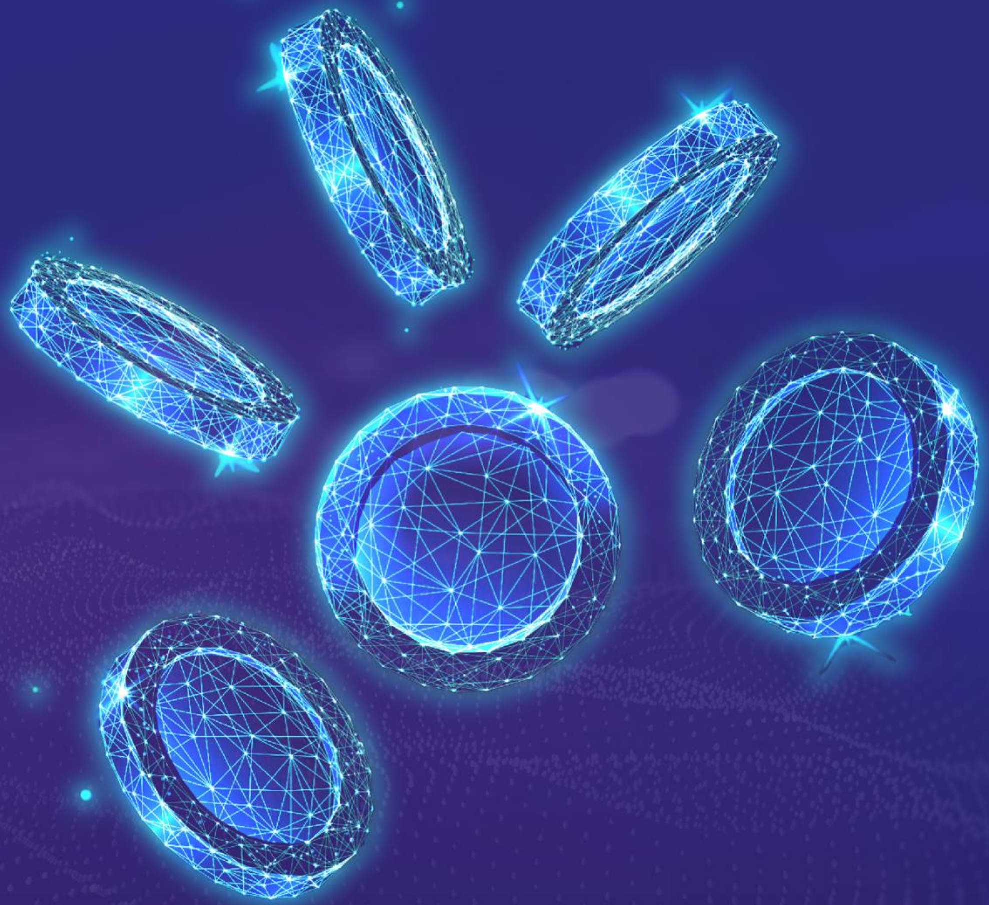
QUOINTELLIGENCE

ENTERTAINMENT

THREAT LANDSCAPE REPORT

2025 – Q2



The Threat Landscape Pyramid

Threats targeting everybody

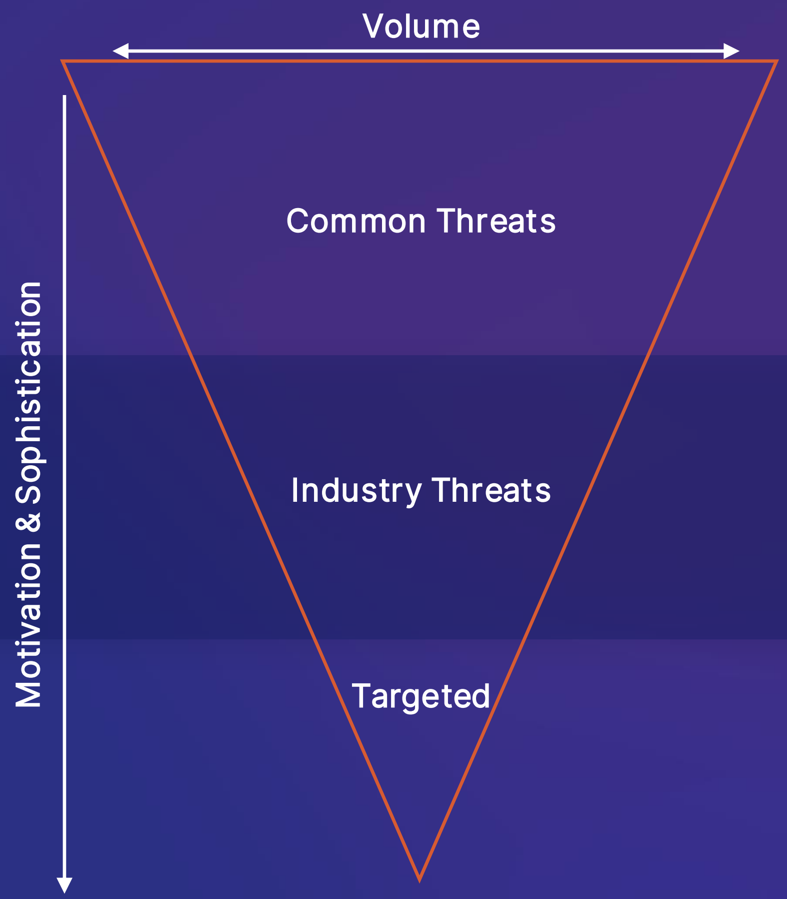
- Malware / Ransomware
- Phishing / Scam
- Worms

Threats targeting specific Industry Sectors

- Banking Trojans
- SCADA malware

Threats targeting specific organizations

- Spear Phishing
- Watering hole
- APT



Examples

- Information Stealers
- Script-kiddies
- Autopwning

- Magecart (e-Commerce)
- Hacktivism (Financial, Gov)
- DragonFly, APT33 (Energy)

- Industrial Espionage
- Insider Threats
- Sabotage

Common Threats Shaping the Quarter

Phishing

AI Generated Content

▬

Ransomware

Extorsions

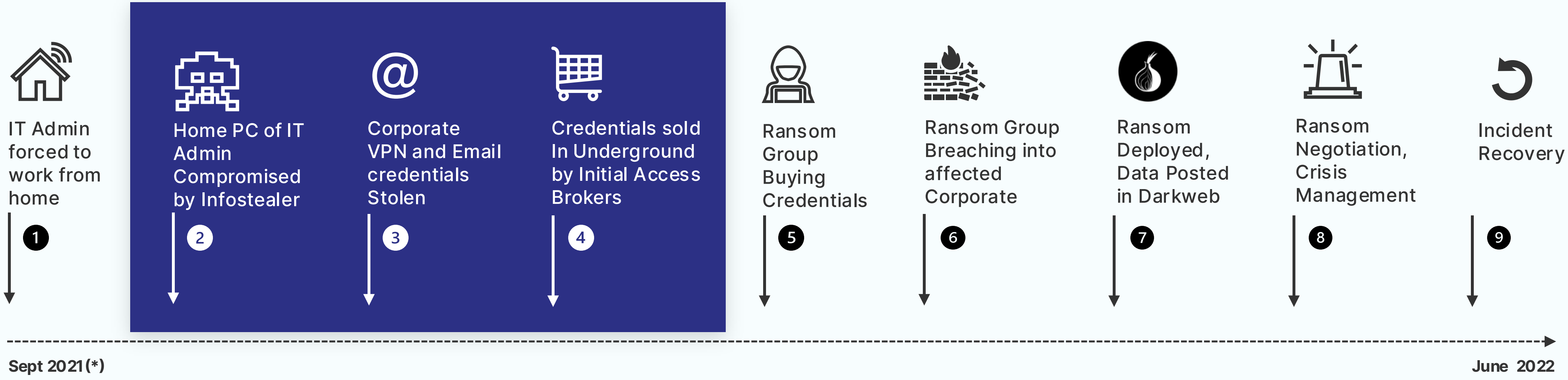
▲▲

Infostealers

▲

Why Common Threats Matter
Ransomware Attack Timeline

***Attack Timeline – Real Example from QuoIntelligence Threat Intelligence-driven IR support activity**



1 IT Admin forced to work from home

2 Home PC of IT Admin Compromised by Infostealer

3 Corporate VPN and Email credentials Stolen

4 Credentials sold In Underground by Initial Access Brokers

5 Ransom Group Buying Credentials

6 Ransom Group Breaching into affected Corporate

7 Ransom Deployed, Data Posted in Darkweb

8 Ransom Negotiation, Crisis Management

9 Incident Recovery

Sept 2021 (*)

June 2022

- **>90% of Data Breaches initiated by by INFOSTEALERS, or MASS-EXPLOITATION**

Targeted Threats Against the Gambling Sector

Phishing Fraud

▲▲

Hacktivism

▼

Ransomware

—

Q1 2025 to Q2 2025 Trends

The gambling sector remains the most attractive target for **fraudulent** activities derived from cybercriminals and **North-Korean state-sponsored adversaries** who exploit trusted communication channels and business routines through customized **phishing and social engineering campaigns** involving platforms like Zoom.

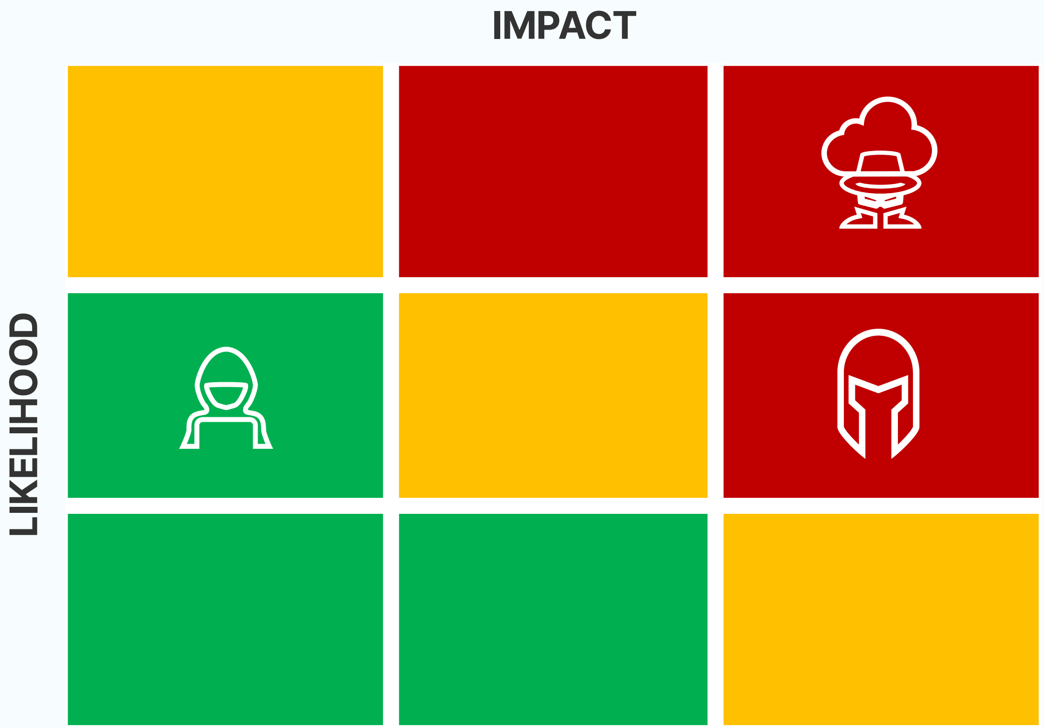
Ransomware remains an opportunistic threat to the gambling sector. No significant increase was recorded in Q2, with activity levels remaining relatively stable and consistent with those seen in the previous quarter.

Due to mainly ideological motives, **hacktivism** and its coordinated cyberattacks remained active during the last quarter. Despite the limited impact such attacks causing a temporary denial of service to customers, these attacks can still result in both a financial loss and brand reputation damage to the company.

Observed Increase of Attacks Targeting the European Gambling Sector

Adversary Type	Risk	Description
Opportunistic Adversaries Financial Fraud Supply Chain Attacks	H	▪ The ransomware threat remains largely opportunistic, though cases in the gambling sector have surfaced, such as reported intrusions on **LeoVegas AB** by **Hellcat** and **Modulus Group** by the **Crypto24** ransomware group. ▪ Several threat actors have leaked data and published database dumps related to European iGaming and casino companies on underground forums. For instance, the threat actor **PrivilegesGenius** advertised a Malta-based casino database on the XSS forum. ▪ **Deepfake** and AI-generated identity fraud are increasingly targeting iGaming onboarding processes, with synthetic applicants bypassing KYC.
State-Sponsored Adversaries Money Laundering Financial Fraud	H	▪ **BlueNoroff** has been linked to phishing and malware campaigns impersonating trusted platforms like Zoom to infiltrate companies, including those in the gambling sector. ▪ Cloudflare's DDoS report ranked the gambling and casino industry among the top five most targeted globally. Of those who identified the attackers, a 21 percent pointed to state-sponsored actors.
Motivated Adversaries Hacktivist Groups	L	▪ Although no significant attacks were observed against the gambling sector during Q2, the opportunistic and indiscriminate nature of ongoing hacktivist-led DDoS campaigns keeps the gambling industry at continued risk especially originating from pro-Palestine hacktivist groups.

Risk Matrix
European Gambling



RISK LEVEL: HIGH

- Hacktivism
- State-Sponsored
- Ransomware, Supply Chain, Fraud

Risk: 🟩 Low 🟨 MEDIUM 🟥 HIGH

Top 10 MITRE ATT&CK Techniques Observed by QuoIntelligence in Gambling Sector Incidents

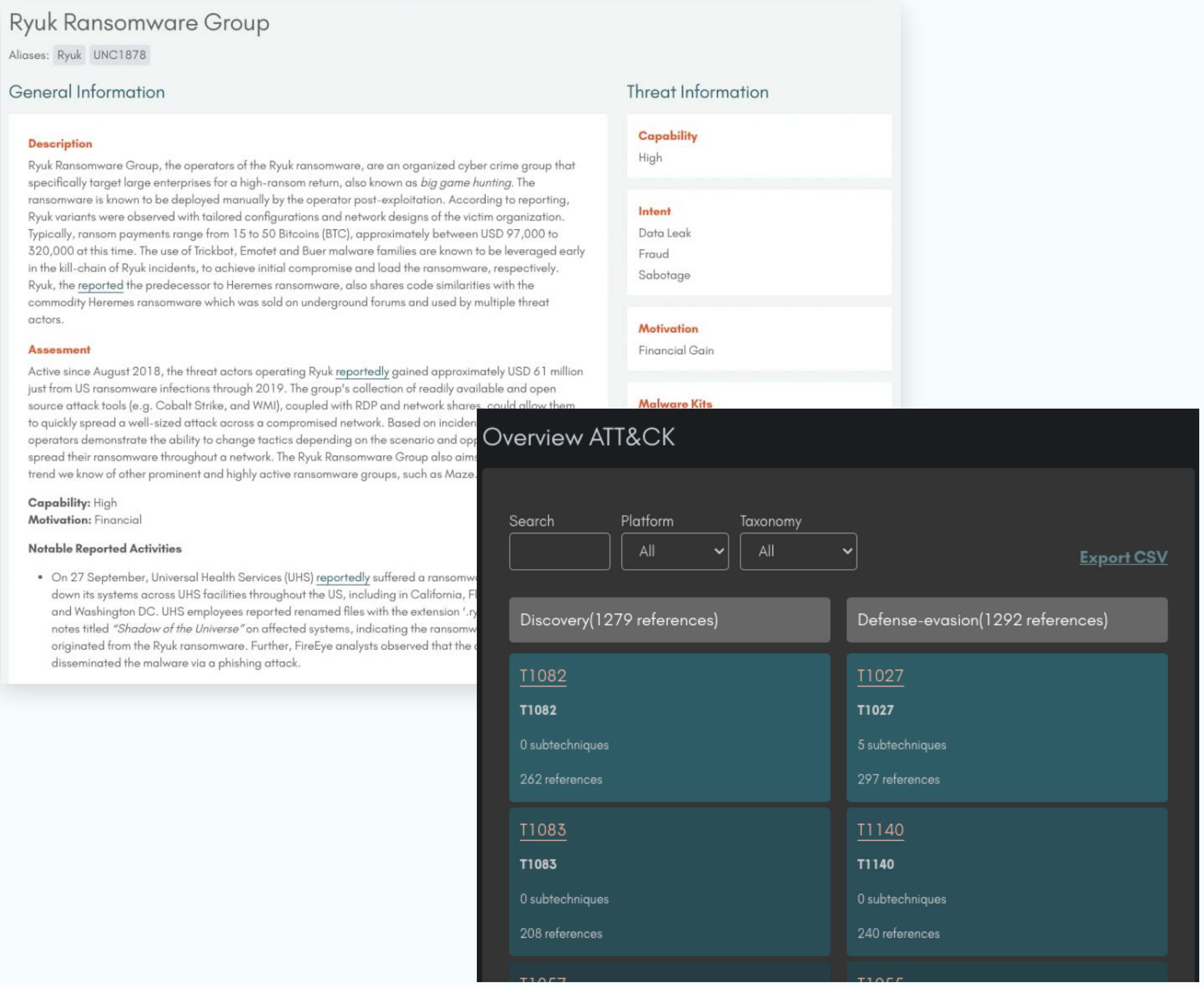
Tactic	Technique	Sub-technique
Initial Access	Spearphishing Link	
Defense Evasion, Execution	Scripting	
Command and Control	Data Obfuscation	Steganography
Discovery	System Network Connections Discovery	
Lateral Movement	Lateral Tool Transfer	
Discovery	Application Window Discovery	
Persistence	Server Software Component	Web Shell
Defense Evasion	Reflective Code Loading	
Reconnaissance	Gather Victim Network Information	
Initial Access, Lateral Movement	Replication Through Removable Media	

🟩 **Less Observed**	🟨	🟥 **More Observed**

Most Used Techniques

- QuoIntelligence tracks more than 150 Threat Actor groups and 480 Attack tools.
- QuoIntelligence profiles all the TTPs (MITRE ATT&CK framework) used by the Threat Actors in our data base.
- QuoIntelligence provides information on how to detect and mitigate these TTPs.

ARE YOU PROTECTED AGAINST THEM?



Ryuk Ransomware Group

Aliases: Ryuk UNC1878

General Information

Description

Ryuk Ransomware Group, the operators of the Ryuk ransomware, are an organized cyber crime group that specifically target large enterprises for a high-ransom return, also known as *big game hunting*. The ransomware is known to be deployed manually by the operator post-exploitation. According to reporting, Ryuk variants were observed with tailored configurations and network designs of the victim organization. Typically, ransom payments range from 15 to 50 Bitcoins (BTC), approximately between USD 97,000 to 320,000 at this time. The use of Trickbot, Emotet and Buer malware families are known to be leveraged early in the kill-chain of Ryuk incidents, to achieve initial compromise and load the ransomware, respectively. Ryuk, the reported the predecessor to Heremes ransomware, also shares code similarities with the commodity Heremes ransomware which was sold on underground forums and used by multiple threat actors.

Assesment

Active since August 2018, the threat actors operating Ryuk reportedly gained approximately USD 61 million just from US ransomware infections through 2019. The group's collection of readily available and open source attack tools (e.g. Cobalt Strike, and WMI), coupled with RDP and network shares, could allow them
to quickly spread a well-sized attack across a compromised network. Based on inciden
operators demonstrate the ability to change tactics depending on the scenario and opp
spread their ransomware throughout a network. The Ryuk Ransomware Group also aims
trend we know of other prominent and highly active ransomware groups, such as Maze.

Capability: High
Motivation: Financial

Notable Reported Activities

- On 27 September, Universal Health Services (UHS) reportedly suffered a ransomw
down its systems across UHS facilities throughout the US, including in California, Fl
and Washington DC. UHS employees reported renamed files with the extension '.ry
notes titled *"Shadow of the Universe"* on affected systems, indicating the ransomw
originated from the Ryuk ransomware. Further, FireEye analysts observed that the c
disseminated the malware via a phishing attack.

Threat Information

Capability
High

Intent
Data Leak
Fraud
Sabotage

Motivation
Financial Gain

Malware Kits

Overview ATT&CK

Search:
Platform: All
Taxonomy: All

Discovery(1279 references)	Defense-evasion(1292 references)
T1082 **T1082** 0 subtechniques 262 references	T1027 **T1027** 5 subtechniques 297 references
T1083 **T1083** 0 subtechniques 208 references	T1140 **T1140** 0 subtechniques 240 references

Regulations Demanding Threat Intelligence

GDPR	▪ Under the **GDPR**, all businesses processing data linked to EU citizens must have a security framework in place to prevent sensitive data breaches. The implementation of threat Intelligence can automatize and bolster these safety countermeasures.
EU’S DIGITAL SERVICES ACT (DSA)	▪ The **DSA** mandates that all online platforms promptly remove any content deemed illegal under EU law. This includes illegal gambling operations, advertising promoting unlicensed gambling services, and also advertising making illegal use of a trademark.

THREAT INTELLIGENCE

GET IN TOUCH

Interested in knowing more about the current Threat Landscape impacting your industry and how you could reduce the risk posed by it?

Book a follow-up meeting
with our experts now!

🌐 quointelligence.eu ✉ curious@quointelligence.eu

QUOINTELLIGENCE