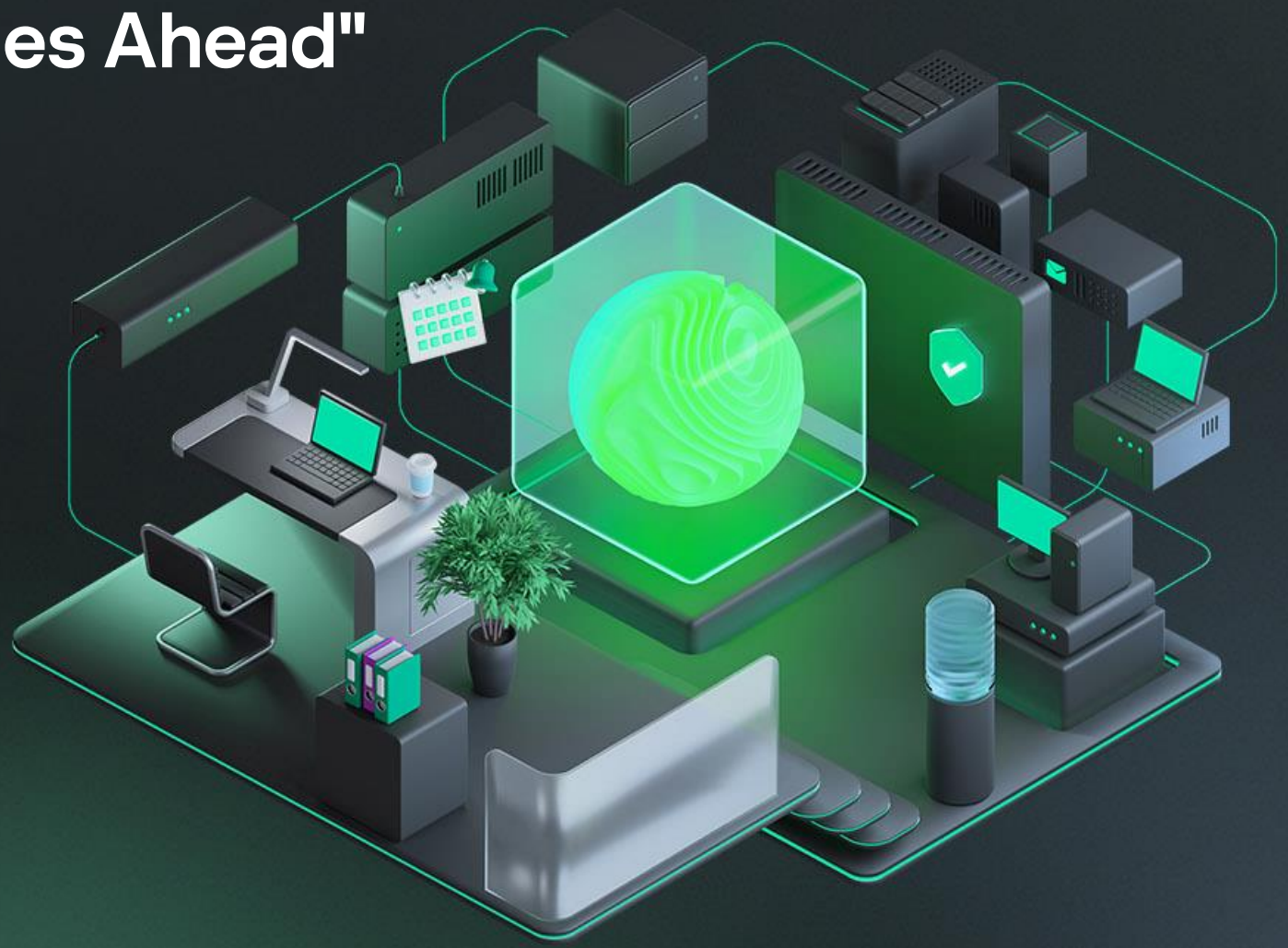
Kaspersky Cybersecurity Trends and Projections:

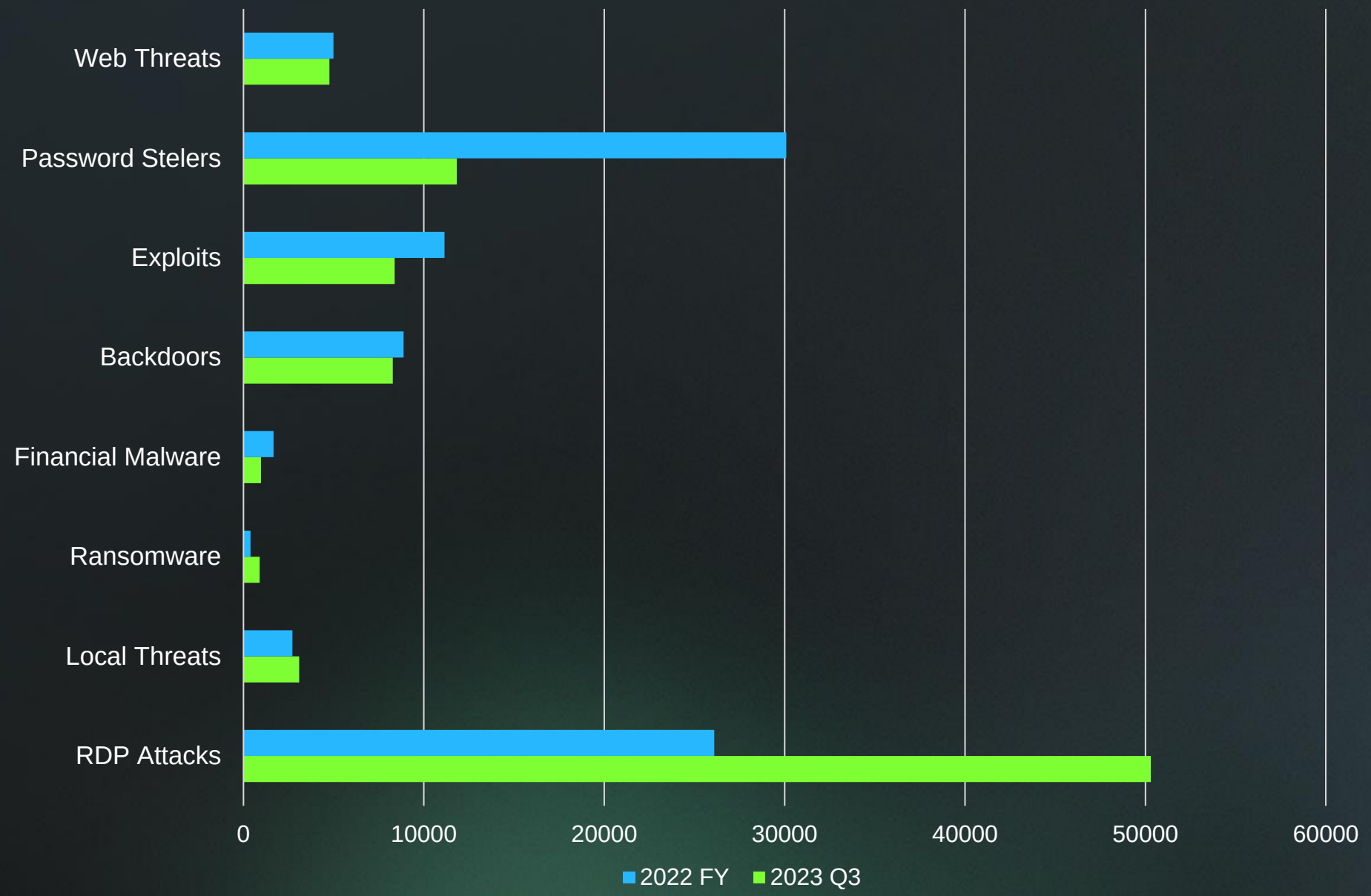
A Year in Review and What Lies Ahead"



Srđan Gligorić, 23.11.2023.

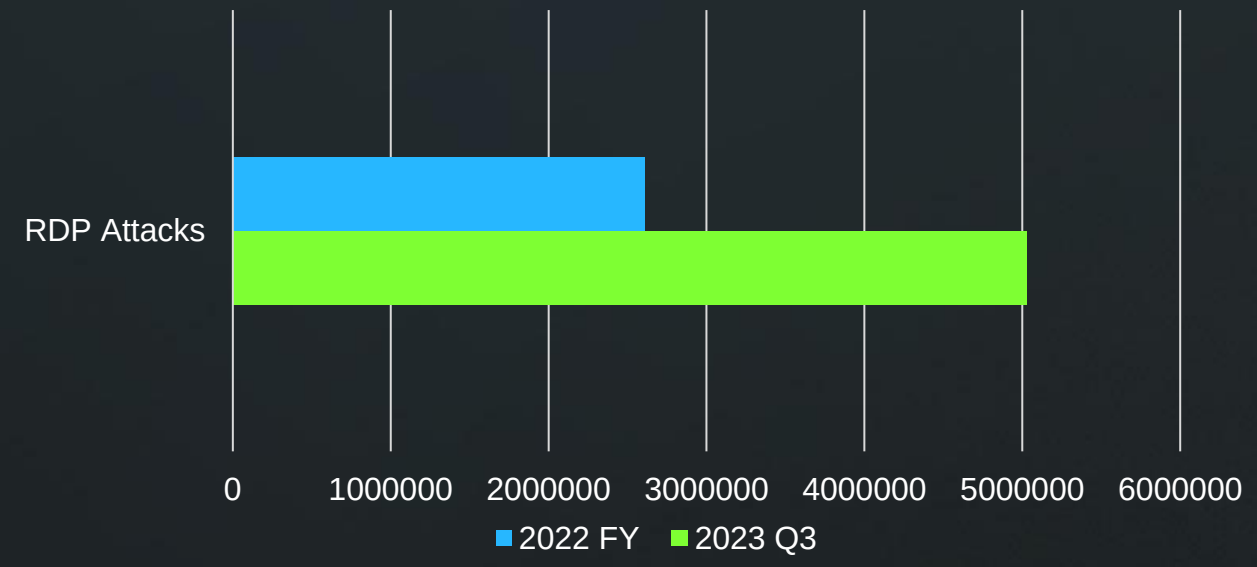
Source of intel data – Kaspersky Security Network & Kaspersky Threat Intelligence

Tipovi pretnji **Srbija 2022 FY – 2023 Q3**



Source of intel data – Kaspersky Security Network & Kaspersky Threat Intelligence

RDP i Ransomware napadi **Srbija 2022 - 2023**



Povećanje **92%** *RDP baziranih napada*

Povećanje **130%** *Ransomware napada*

Trojan-Ransom.Win32.Stop.gen

Trojan-Ransom.Win32.Encoder.pef

Trojan-Ransom.Win32.Gen.gen

Trojan-Ransom.Win32.Stop.gen

Trojan-Ransom.Win32.Wanna.zbu

Trojan-Ransom.Win32.Phobos

RDP napadi

1. Skeniranje i pretraživanje otvorenih RDP portova
2. Napadi grubom silom (Brute force attack)
3. Popunjavanje akreditiva korišćenjem kompromitovanih naloga
4. Čovek u sredini (MITM) napadi sa krađom podataka
5. Otmica sesije – preuzimanje kontrole nad već uspostavljenom RDP sesijom
5. BlueKeep ranjivost

Najbolje bezbednosne prakse:

1. Korišćenje jakih, jedinstvenih lozinki (Kaspersky Password Manager)
2. Primena višefaktorske autentifikacije,
3. Ažuriranje softvera i sistema sa bezbednosnim zakrpama i ograničavanje pristupa RDP-u samo na neophodne korisnike i IP adrese.

Mrežni zaštitni zidovi i sistemi za otkrivanje/prevenciju upada (Kaspersky XDR) mogu pomoći u smanjenju rizika od RDP napada!!!

Incident response – najčešći odgovor od strane analitičara Kasperskog

“The files have been encrypted by Trojan-Ransom.Win32.Phobos. Unfortunately, this malware variant uses a cryptographically secure algorithm so decryption is not possible without the threat actors' private key.

According to data collected the criminals used RDP brute-force to infect the victim, therefore, please change the RDP passwords to avoid a recurring infection.

Additionally, we recommend to avoid opening access to RDP from the Internet, and to use VPN to connect to the corporate network instead.”

7,000,000,000

Sajber napada

Detektovano od strane Kasperskog u 2022

400,000

Novih malicioznih fajlova

Detektuje Kaspersky svaki dan

Advanced persistent threat napadi u 2022-oj

Kaspersky's Global Research and Analysis Team (GReAT) je vodeća svetski tim za analizu i otkrivanje najnaprednijih sajber napada. Prema našim podacima, u 2022-oj vodeće APT mete su bile državne institucije a najaktivnija grupa je bila Lazarus.

Top 10 vertikala

- Government
- Military
- Diplomatic
- IT companies
- Educational
- Telecommunications
- Media
- Software Development
- Manufacturing
- Logistics

Top 10 najznačajnijih grupa

1. Lazarus
2. APT10
3. Kimsuky
4. ZexCone
5. Tomiris
6. Ghostwriter
7. DeathStalker
8. BitterAPT
9. SideCopy
10. Gelsemium

Top 12 targetiranih zemalja

apt.securelist.com

Based on the data up to 31.12.2022

Operacija TRIANGULACIJA – koliko koristimo IOS uređaje kao službene uređaje u državnoj upravi?

Operation TRIANGULATION (2023) - Advanced Persistent Threat (APT) kampanja koja je ciljala iOS uređaje

- IOS uređaji imaju zatvoren sigurnosni sistem koji onemogućava instaliranje IT bezbednosnih alata (zaštitne mere ugrađene su u IOS i na hardverskom (na nivou Apple čipova kod novih uređaja) i na softverskom nivou
- Sofisticiran metod distribucije eksploita putem „zero-click“ iMessage poruka korišćen u kampanji
- Preuzimanje kompletne kontrole nad uređajem i svim podacima korisnika
- Zbog kompleksnosti napada i zatvorene strukture IOS ekosistema, dediciran multidisciplinarni tim inženjera proveo je dosta vremena detaljno analizirajući ovaj napad
- Kampanja otkrivena uz pomoć alata za analizu mrežnog saobraćaja
- Pet ranjivosti (od čega četiri „zero-day“) koje su korišćene u kampanji su uklonjene od strane Apple-a nakon istraživanja od strane Kaspersky inženjera
- Targetirani zasposleni kompanije Kaspersky, zaposleni u vladinom sektoru kao i „zanimljivi pojedinci“
- Kaspersky je razvio alate za analizu i detekciju ovog napada koji su na raspolaganju svima

Da biste saznali više posetite: Securelist.com

Extended Detection and Response (XDR)

XDR, tehnologija naslednica EDR-a (Endpoint Detection and Response), je moderan bezbednosni pristup koji se bazira na skupljanju velike količine sigurnosnih podataka i analizi iz različitih izvora kako bi se zatvorio jaz i zaokružila vidljivost i osigurao uvid u maliciozne aktivnosti kroz ceo spektar IT/OT sistema.

Kaspersky XDR – jedna platforma za prevenciju, detekciju i odgovor na sve pretnje

KasperskyOS je efektivna platforma za razvoj Sajber imunih proizvoda

Microkernel OS za IT sisteme sa visokim zahtevima informacione bezbednosti

- Pruža platformu za kreiranje secure-by-design rešenja
- Kreira okruženje koje ne dozvoljava aplikacijama da izvršavaju nedeklarisane funkcije i sprečava iskorišćenja ranjivosti
- Pruža punu transparentnost, fleksibilnu konfiguraciju bezbednosnih polisa i kontrolu nad interakcijama u okviru kompletnog sistema

KasperskyOS portfolio rešenja

Kaspersky IoT Infrastructure Security

A solution for cybersecure data transfer to digital and cloud business platforms, as well as for infrastructure protection and transparency

- Kaspersky IoT Secure Gateway
- Kaspersky Security Center

Kaspersky Secure Remote Workspace

A solution for building a Cyber Immune, functional, and manageable thin client infrastructure with convenient, centralized management

- Kaspersky Thin Client
- Kaspersky Security Center
- Kaspersky Security Management Suite

Kaspersky Automotive Secure Gateway

Building reliable IT systems for smart road vehicles

- Kaspersky Automotive Adaptive Platform
- Kaspersky Automotive Secure Broker Framework
  - Kaspersky OTA Agent
  - Kaspersky Vehicle SOC Agent
  - Kaspersky Remote Diagnostic Agent

POWERED BY KasperskyOS

Kaspersky Enterprise Rešenja

Targetirana rešenja

- Kaspersky Industrial CyberSecurity
- Kaspersky Fraud Prevention
- Kaspersky Research Sandbox
- Kaspersky Threat Attribution Engine
- Kaspersky Private Security Network
- Kaspersky IoT Embedded Security

Stage 3

Complex and APT-like attacks

Expert Security

Mature IT security capability or a SOC team

- **Internal Expertise**
  - Kaspersky Cybersecurity Training
- **Intelligence**
  - Kaspersky Threat Intelligence
- **Extended Detection and Response**
  - **Native XDR**
    - Kaspersky Endpoint Detection and Response Expert
    - Kaspersky Anti Targeted Attack
  - **Open XDR**
    - Kaspersky Extended Detection and Response
- **SIEM**
  - Kaspersky Unified Monitoring and Analysis Platform
- **External Guidance**
  - Kaspersky Incident Response
- **Assessment**
  - Kaspersky Security Awareness Ultimate

Stage2

Evasive threats

Optimum Security

IT Security

- **Visibility and response**
  - Kaspersky Endpoint Detection and Response Optimum
- **Containers**
  - Kaspersky Container Security
- **Detection Enrichment**
  - Kaspersky Threat Intelligence Portal
- **People**
  - Kaspersky Security Awareness Advanced

Stage 1

Commodity Threats

Security Foundations

IT

- **Endpoint**
  - Kaspersky Endpoint Security for Business
  - Kaspersky Embedded Systems Security
  - Kaspersky Hybrid Cloud Security
- **Network**
  - Kaspersky Security for Mail Server
  - Kaspersky Security for Internet Gateway
- **Data**
  - Kaspersky Security for Storage
- **Support**
  - Kaspersky Premium Support and Professional Services

Kaspersky Managed Detection and Response

HVALA NA PAŽNJI !

Srdjan.Gligoric@Kaspersky.com