CYBERSECURITY IN THE FACE OF MODERN THREATS: FROM RANSOMWARE TO DATA PROTECTION

Bucharest – 11th of October 2024

Daniel-Florin PITIS

ABOUT ME

- **Secure Coding Specialist** @Edenred Digital Center since 2020
- Software Development Background, specialized in Application Security, Training & Awareness
- Volunteering @SecurityPatch.ro project
- Speaker at Forum in Cyber, BSides, Cybersecurity Dialogues

YOU WANT TO BE PART OF OUR TEAM?

- We are looking for new colleagues to join our security team in Bucharest:

Information Security Specialist

IT Crisis Management Expert

- Check all our opened positions here

Spitalele din România afectate d ransomware

Campanii · Gabriel Puiu · februarie 17, 2024

Articol scris de Gabriel Puiu

Ce s-a întâmplat?

Pe data de 12 februarie 2024 Directoratul Național de Securitate Cibernetică a publicat un comunicat de presă în care anunța că o companie ce furnizează software-ul pentru mai multe spitale din România a fost vizată de un atac cibernetic de tip ransomware. Este vorba despre compania Romanian Soft Company, companie românească, producătoare de software HIS (Hospital Information System).

Înființată în anul 2000, compania Romanian Soft Company furnizeaza software-ul Hipocrate către multiple spitale din România, dintre care, conform altui comunicat DNSC, 26 au fos
software de tip HIS, în cadrul căruia se centraliz
date financiare etc. Pe lângă aceste lucruri, aces
sau Ministerul Sănătății.

Lista celor 21 de spitale afectate nu a fost însă li
autorități, în acest moment fiind confirmate în to
alte 79 unități din sistemul de sănătate au fos
acestora din urmă, atacatorii nu s-au identifi
răscumpărare în afară de o adresă de email și co

Presa internațională a preluat foarte rapid știrea
atacului și punând securitatea unităților de sănăt

Backmydata Ransomwa

Conform DNSC, malware-ul utilizat în cadrul at
Phobos, cunoscută pentru propagarea prin cone

Phobos este un Ransomware-as-a-Service (Raa
organizațiilor, scammeri, script kiddies, terți ha
răscumpărării.

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

Cauta

Amenințări Alerte Învățământ Directiva NIS Conștientizare Evenimente

ALERTĂ: Backmydata Ransomware - Indicatori compromitere (IOCs)

2024/02/15 Popularitate 1116 Postează

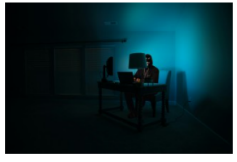


Foto: Clint Patterson (Unsplash)

În cursul nopții de 11 spre 12 februarie 2024 a cibernetic de tip ransomware asupra companie Company (RSC) www.rsc.ro care dezvoltă, adr comercializează sistemul informatic **Hipocrate** datelor DNSC, atacul a perturbat activitatea a 2 care utilizează sistemul informatic **Hipocrate**.

Malware-ul utilizat în cadrul atacului este **aplic Backmydata** care face parte din **familia de malware Phobos**, cunoscută pentru propagarea prin conexiuni de tip **Remote Desktop Protocol (RDP)**. **Backmydata** este conceput pentru a cripta fișierele țintei vizate utilizând un algoritm complex. Fișierele criptate sunt redenumite cu extensia **.backmydata**. După criptare, malware-ul furnizează **două note de răscumpărare** (**info.hta** și **info.txt**) cu detalii despre pașii de urmat pentru contactarea atacatorilor și stabilirea detaliilor pentru plata răscumpărării.

DNSC recomandă tuturor entităților din domeniul sănătății, indiferent dacă au fost sau nu afectate de atacul ransomware Backmydata, să scaneze infrastructura proprie IT&C prin utilizarea scriptului de scanare YARA.

Municipiul Timișoara

Servicii

Acasă › Noutăți

26 August 2024

Primăria Timișoara a oprit un atac cibernetic masiv asupra serverelor sale și ale unor instituții subordonate

Primăria Municipiului Timișoara, Direcția Fiscală a Municipiului (DFMT) și Poliția Locală Timișoara au fost țintă unui atac cibernetic de tip ransomware asupra serverelor pe care rulează mai multe sisteme informatice.

Incidentul a avut loc în noaptea de vineri spre sâmbătă și a fost detectat de sistemul digital de securitate. Specialiștii primăriei au declanșat o serie de contra-măsuri radicale, cu ajutorul firmelor de specialitate contractate de municipalitate, astfel că a fost oprită compromiterea întregului sistem. Nu există indicii că atacatorii au extras date cu caracter personal din sistemele afectate.

ȘTIRI · AGORA · EXPLORE · RUBRICA DE AI

nătate din Florida, primul sistem de sănătate publică acreditat din Statele Unite, a căzut somware de către grupul notoriu RansomHub. Atacatorii susțin că au accesat un volum de izaționale și amenință să publice informațiile furate în următoarele trei-patru zile. Printre

de breșe sunt potențial devastatoare, având în vedere natura sensibilă a datelor deținute de ătate din Florida.

nsabilă pentru o gamă largă de servicii de sănătate publică, de la prevenirea bolilor și până la pregătirea și răspunsul la urgențe.

O scurgere de date de această magnitudine ar putea expune informații personale, ar putea perturba serviciile de sănătate și ar putea submina încrederea publicului în sistemul de sănătate al statului.

Breșă de Dat

Simultan un lider global în servicii de afaceri și tehnologie, a fost, de asemenea, țintă grupului RansomHub.

Grupul de hackeri susține că a accesat 230 GB de date de la divizia română i că intenționează să le publice

Three key points we will cover today to better understand the phenomenom and stenghten our protection

1

Ransomware & RaaS

2

Statistics

3

How can we protect ourselves?

1.

Ransomware & RaaS

WHAT IS RANSOMWARE?

- Is a type of malicious software or malware that threatens a victim by destroying or blocking access to critical data or systems, until a **ransom is paid**

Some of the attackers use internal financial documents they have discovered to set up ransom price

WHAT IS RAAS?

Ransomware as a service (RaaS) is a cybercrime business model in which ransomware developers sell ransomware code or malware to other hackers, called "affiliates" who then use the code to initiate their own ransomware attacks

- **Monthly subscription –** RaaS affiliates pay a recurring fee for access to ransomware tools
- **One-time fee –** Affiliates pay a one-time fee to purchase the ransomware code outright
- **Affiliate Programs –** Affiliates pay a monthly fee and share a small % of any ransom payments that they receive with the operators
- **Profit Sharing –** The operators charge nothing up front, but take a significant cut of every ransom the affiliate receives (usually 30-40%)

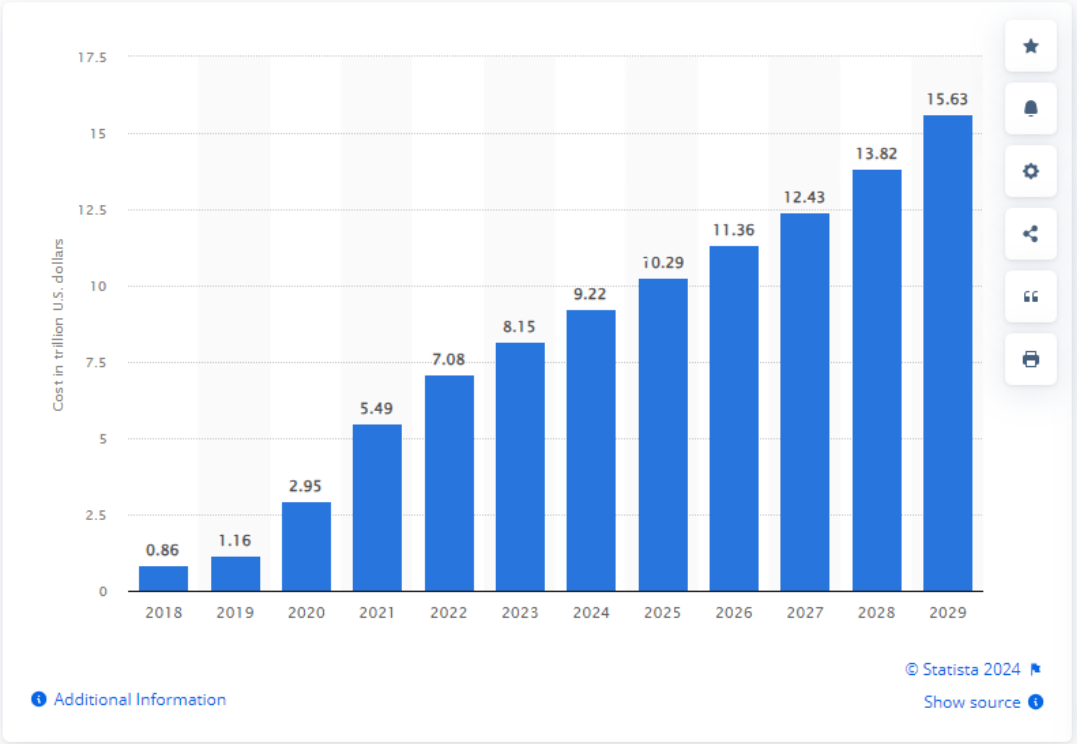
2.

Statistics

COST OF CYBERCRIME

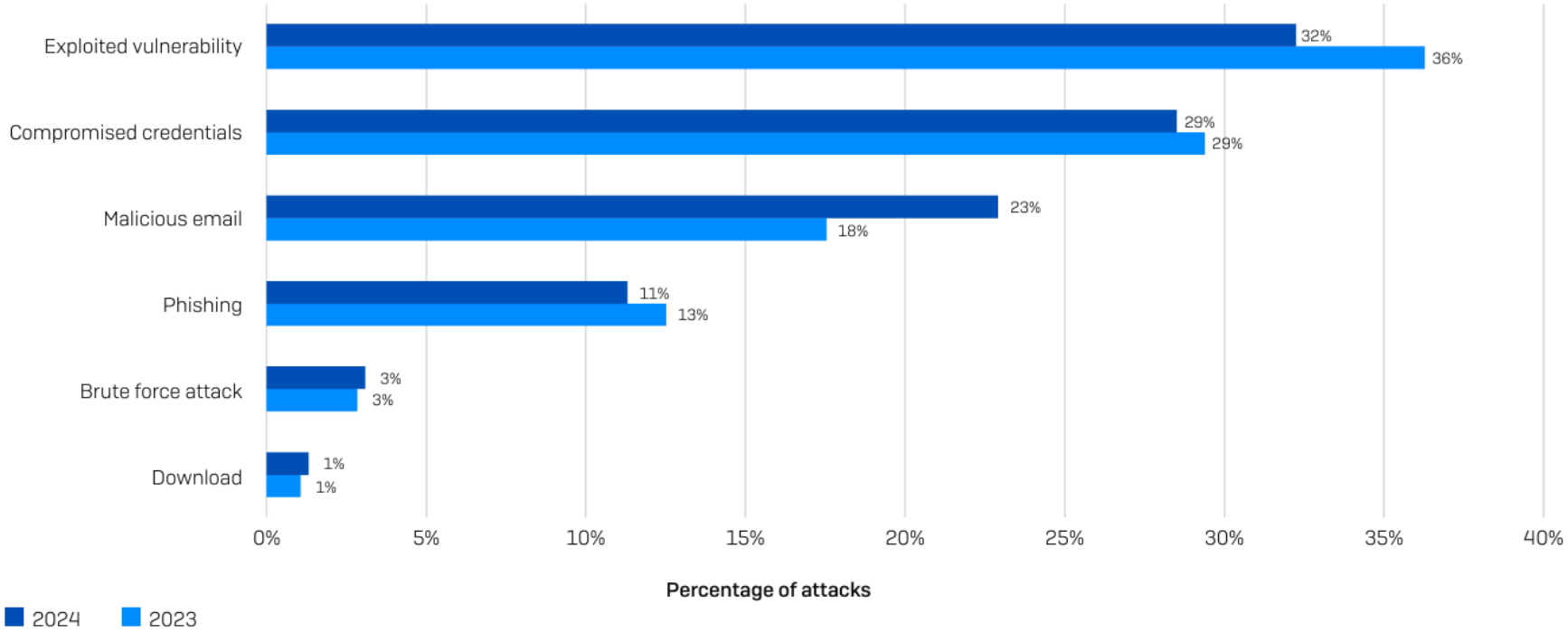
Estimated cost of cybercrime worldwide 2018-2029

(in trillion U.S. dollars)



1. https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

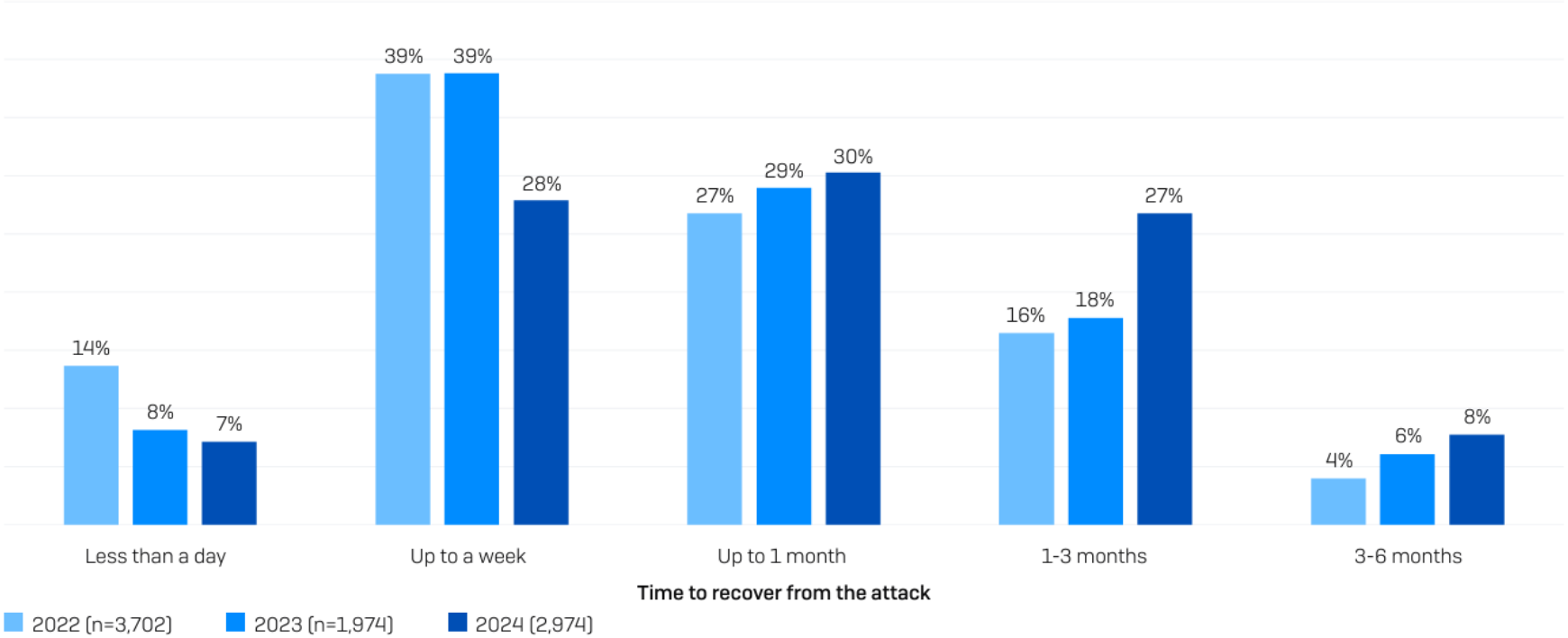
ROOT CAUSE OF RANSOMWARE ATTACKS IN 2024



Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. n=2,974 organizations hit by ransomware.

1. The State of Ransomware 2024 (Sophos)

TIME TO RECOVER FROM THE ATTACK



How long did it take your organization to fully recover from the ransomware attack? Base number in chart.

1. *The State of Ransomware 2024 (Sophos)*

3.

How can we protect ourselves?

How can we protect ourselves?

The “No More Ransom” website initiative - https://www.nomoreransom.org/

01

Cybersecurity Training & Awareness

Educate employees about the risks of ransomware and how to identify phishing attempts, which are common entry points for the attackers

02

Maintaining backups

Regular backups of critical data is one of the most effective defense against ransomware. Ensure that backups are stored offline, or in a cloud service with strong security features

03

Implementing access controls

Utilize the principle of least privilege by restricting user permissions to only what is necessary for their role. Implement MFA for critical systems to add an extra layer of security

04

Working with law enforcement

Law enforcement agencies often have specialized units that deal with cybercrime, and they can provide guidance on investigation process, help track down perpetrators, and offer intelligence about emerging threats

Q&A

Thank you

Enrich
connections.
For good.