SECURITY DAYS

VÝVOJ HROZIEB 2023-2024

Operácia Texonto, trendy, ChatGPT,
MOVEit, AceCryptor-Rescoms, Telekopye

Digital Security
Progress. Protected.

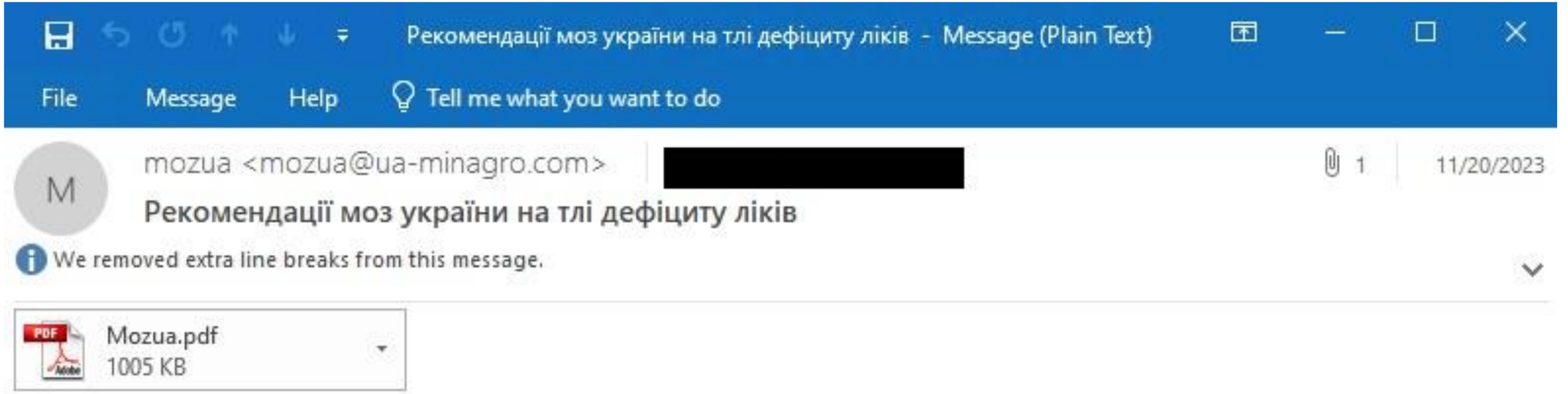
& SME KONFERENCIE

Robert Lipovsky

Principal Threat Intelligence Researcher

@Robert_Lipovsky @Rockouter

Operácia Texonto



Міністерство охорони здоров'я попереджає про дефіцит ліків в аптеках — доставка деяких препаратів на тлі підвищеного попиту може затримуватися.

З початком війни з РФ Україна повністю відмовилася від лікарських засобів російських і білоруських фармацевтичних компаній, доходи населення впали, а іноземні ліки, логістика яких змінилася і стала більш складною і вартісною, значно подорожчали. При цьому, найбільшим попитом у громадян України користуються групи препаратів для лікування хронічних захворювань, заспокійливі, знеболюючі та хірургічні засоби.

На тлі виниклого дефіциту МОЗ України нагадав громадянам, що не варто нехтувати безцінним досвідом перевірених століттями народних методів лікування і випустив відповідні рекомендації.

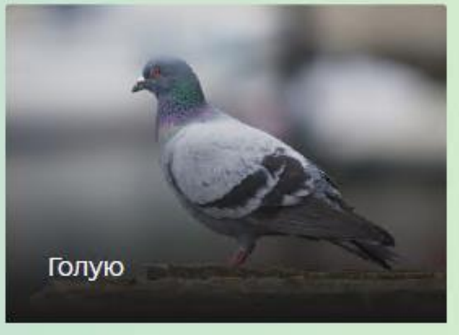
МІНІСТЕРСТВО АГРАРНОЇ ПОЛІТИКИ ТА ПРОДОВОЛЬСТВА УКРАЇНИ

Шановні громадяни!

Рецепти України

Агресія Росії призвела до значних втрат в аграрному секторі України. Землі забруднені мінами, пошкоджені снарядами, окопами і рухом військової техніки. У великій кількості пошкоджено та знищено сільськогосподарську техніку, знищено зерносховища. До стабілізації обстановки Міністерство аграрної політики та продовольства рекомендує вам урізноманітнити раціон стравами з доступних дикорослих трав. Вживання свіжих, соковитих листя трав у вигляді салатів є найбільш простим, корисним і доступним. Пам'ятайте, що збирати рослини слід далеко від міст і селищ, а також від жвавих трас. Пропонуємо вам кілька корисних і простих у приготуванні рецептів.

РІЗОТТО З ГОЛУБОМ



Голую

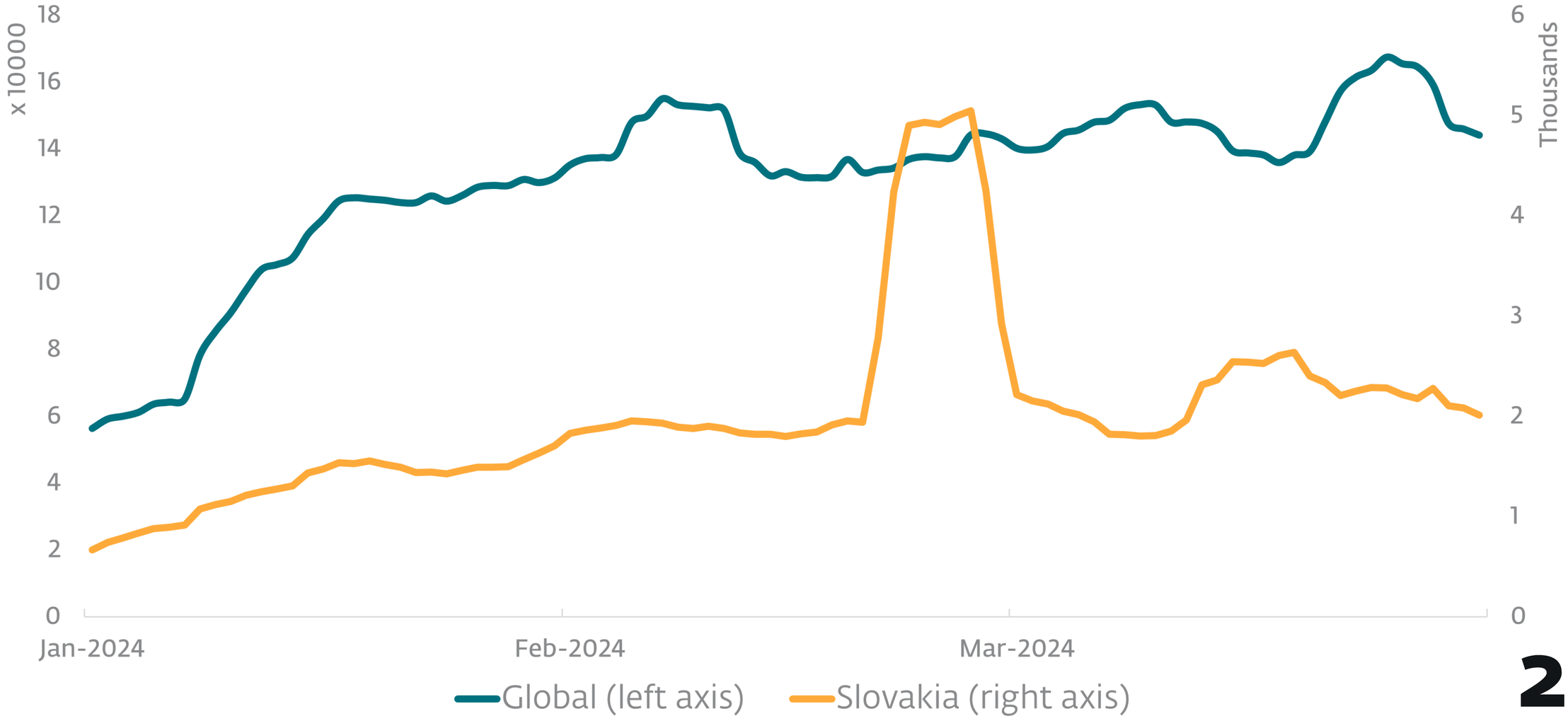
Готове блюдо

Ощипати, обробити і добре промити тушу голуба. У глибокій сковороді розтопити **55 г.** масла. Викласти м'ясо і цибулю. Обсмажити на середньому вогні, періодично помішуючи, протягом **8-10 хв**. до золотистого кольору. Далі знизити вогонь, висипати в сковороду рис, смажити, помішуючи, близько **1-2 хв**. Посолити і поперчити. Варити до повного випаровування рідини. Додати **2 ополоника** води і варити, помішуючи, до випаровування рідини. Всього за часом має піти близько **25** хвилин. Подавати різотто на окремих тарілках, прикрасивши листочками петрушки.

- navalny-votes.net
- navalny-votesmart.net
- navalny-voting.net

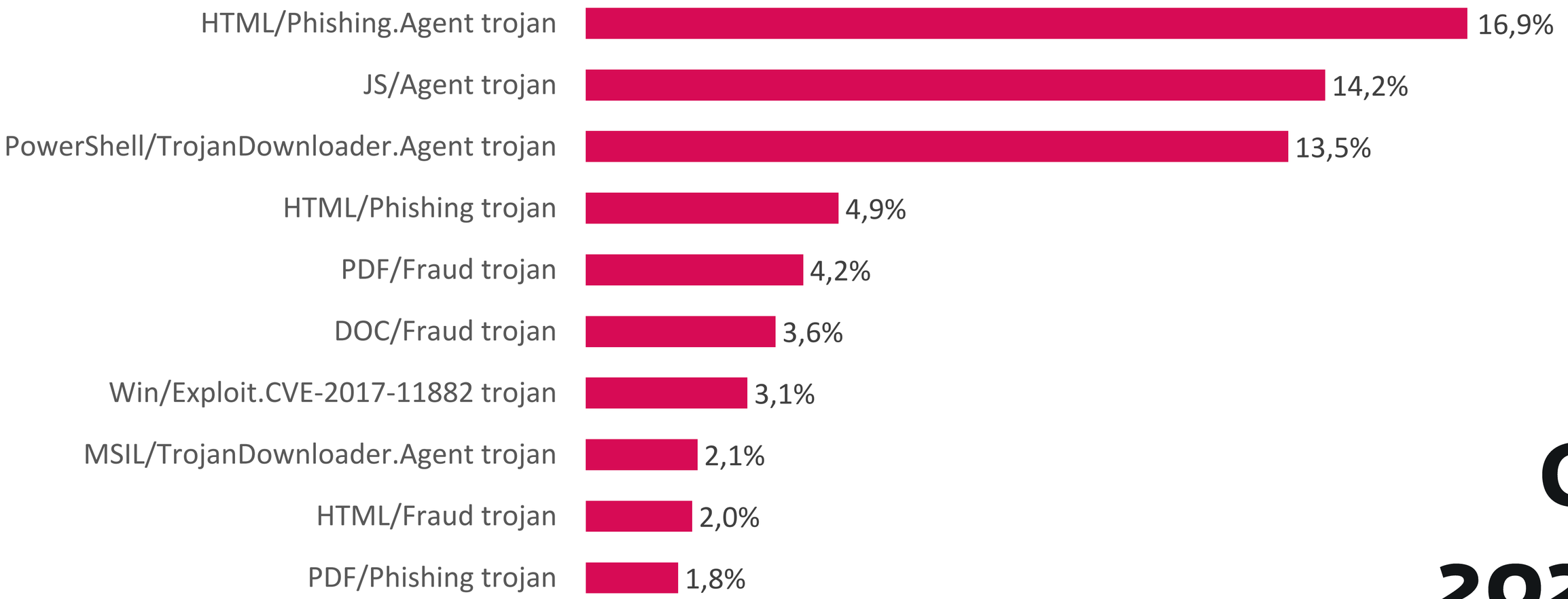
Detekcie a trendy

Trend detekcii – svet vs. Slovensko



Q1 2024

Top 10 detekcií na Slovensku



Q1
2024

JS/Agent globálny nárast

JS/Agent.RAN & .RAW

BLEEPINGCOMPUTER

Search Site LOGIN SIGN UP

NEWS DOWNLOADS VPNS VIRUS REMOVAL GUIDES TUTORIALS DEALS FORUMS MORE

Home > News > Security > Over 17,000 WordPress sites hacked in Balada Injector attacks last month

Over 17,000 WordPress sites hacked in Balada Injector attacks last month

By Bill Toulas October 9, 2023 03:23 PM 1

tagDiv

CVE-2023-3169

Nárast (ne)kvalitných o phishingu

POLICAJNÝ ZBOR SLOVENSKEJ REPUBLIKY

SLOVENSKA REPUBLIKA

Nad Tatrou sa blýska

KONVOKÁCIA

Na účely súdneho vyšetrovania
Súbor N°7288/SK

Som Mjr. JUDr. , podplukovník odboru kriminálnej polície v spolupráci s Európskym policajným úradom (EUROPOL) Vám zasielame túto výzvu po zaistení počítača prostredníctvom kybernetickej infiltrácie (oprávnenej najmä v oblasti detskej pornografie, pedofilie, kybernetickej pornografie, exhibicionizmu, obchodovania s ľuďmi za účelom sexuálneho zneužívania, od roku 2016), aby sme Vás informovali, že ste predmetom viacerých právnych konaní podľa platného Trestného poriadku v oblasti kybernetickej kriminality Skutočnosti sú nasledovné:

PEDOPORNOGRAFIA - PEDOFÍLIA - EXHIBICIONIZMUS - KYBERPORNOGRAFIA - SPRENEVERA PEŇAZÍ

Upozorňujeme, že zákon z marca 2020 sprísňuje tresty v prípade, že k návrhu, sexuálnemu útoku alebo znásilneniu mohlo dôjsť prostredníctvom internetu a vy ste sa uvedených trestných činov dopustili po tom, ako sa na vás zameral náš kybernetický strážnik prostredníctvom toku vašich internetových údajov, ktorý predstavuje dôkaz o vašich trestných činoch.

Preto vás žiadame, aby ste sa vyjadrili e-mailom a napísali nám svoje odôvodnenia, aby sme ich mohli preskúmať a overiť s cieľom posúdiť sankcie, a to v prísne stanovenej lehote 72 hodín. Po uplynutí tejto lehoty budeme povinní odovzdať našu správu kancelárii zástupcu prokurátora súdu prvého stupňa v Créteil, špecialistu na počítačovú kriminalitu, s cieľom vypracovať príkaz na vaše zatknutie, ktorý bude postúpený žandárskej stanici v najbližšom mieste vášho bydliska. Preto budete zaregistrovaný ako sexuálny delikvent a ako sa uvádza v núdzovom postupe, vaše informácie budú zaslané združeniam bojujúcim proti pedofílii a niekoľkým národným televíznym kanálom na hromadné vysielanie, aby sa vaša rodina, vaši priatelia a celé Francúzsko dozvedeli, čo robíte pred počítačom.

Preto očakávame vaše vysvetlenia na týchto adresách: mjr.judr. @gmail.com

Teraz, keď ste boli varovaní, prijmite toto zvolanie za službu a hodnotu.

Mjr. JUDr.
Riaditeľ
odboru kriminálnej polície

SLOVENSKA REPUBLIKA

POLICAJNÝ ZBOR SLOVENSKEJ REPUBLIKY

SLOVENSKA REPUBLIKA

Nad Tatrou sa blýska

KONVOKÁCIA

Na účely súdneho vyšetrovania
Súbor N°7288/SK

Som Mjr. JUDr. , podplukovník odboru kriminálnej polície v spolupráci s Európskym policajným úradom (EUROPOL) Vám zasielame túto výzvu po zaistení počítača prostredníctvom kybernetickej infiltrácie (oprávnenej najmä v oblasti detskej pornografie, pedofílie, kybernetickej pornografie, exhibicionizmu, obchodovania s ľuďmi za účelom sexuálneho zneužívania, od roku 2016), aby sme Vás informovali, že ste predmetom viacerých právnych konaní podľa platného Trestného poriadku v oblasti kybernetickej kriminality Skutočnosti sú nasledovné:

obchodovania s ľuďmi za účelom sexuálneho zneužívania, od roku 2016), aby sme Vás informovali, že ste predmetom viacerých právnych konaní podľa platného Trestného poriadku v oblasti kybernetickej kriminality Skutočnosti sú nasledovné:

PEDOPORNOGRAFIA - PEDOFÍLIA - EXHIBICIONIZMUS - KYBERPORNOGRAFIA - SPRENEVERA PEŇAZÍ

Upozorňujeme, že zákon z marca 2020 sprísňuje tresty v prípade, že k návrhu, sexuálnemu útoku alebo znásilneniu mohlo dôjsť prostredníctvom internetu a vy ste sa uvedených trestných činov dopustili po tom, ako sa na vás zameral náš kybernetický strážnik prostredníctvom toku vašich internetových údajov, ktorý predstavuje dôkaz o vašich trestných činoch.

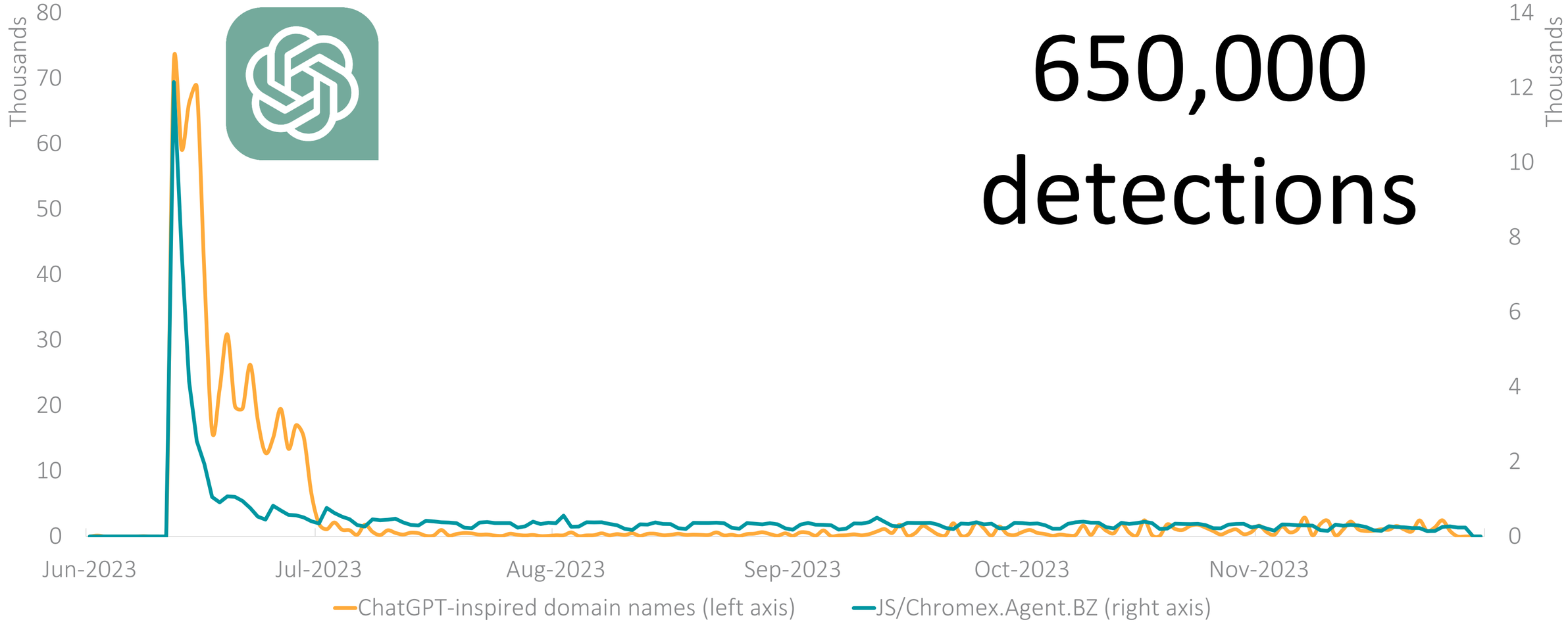
Preto vás žiadame, aby ste sa vyjadrili e-mailom a napísali nám svoje odôvodnenia, aby sme ich mohli preskúmať a overiť s cieľom posúdiť sankcie, a to v prísne stanovenej lehote 72 hodín. Po uplynutí tejto lehoty budeme povinní odovzdať našu správu kancelárii zástupcu prokurátora súdu prvého stupňa v Créteil, špecialistu na počítačovú kriminalitu, s cieľom vypracovať príkaz na vaše zatknutie, ktorý bude postúpený žandárskej stanici v najbližšom mieste vášho bydliska. Preto budete zaregistrovaný ako sexuálny delikvent a ako sa uvádza v núdzovom postupe, vaše informácie budú zaslané združeniam bojujúcim proti pedofílii a niekoľkým národným televíznym kanálom na hromadné vysielanie, aby sa vaša rodina, vaši priatelia a celé Francúzsko dozvedeli, čo robíte pred počítačom.

Preto očakávame vaše vysvetlenia na týchto adresách: mjr.judr.[redacted]@gmail.com

ChatGPT (ako návnada)

Malicious ChatGPT-like domains...

650,000 detections



Detections of malicious ChatGPT-inspired domain names and JS/Chromex.Agent.BZ in H2 2023, seven-day moving average

MOVEit hack: najhorší útok 2023

CVE-2023-34362
severe SQL injection

Bez šifrovania. Len vydieranie

DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

Dlhý zoznam obetí

CL0P^_- LEAKS

HOME HOW TO DOWNLOAD? ARCHIVE INDIABULLS.COM SOFTWAREAG.COM PARKLAND.CA

ELANDRETAIL.COM SYMRISE.COM SINGTEL.COM DANAHER.COM JONESDAY.COM

BOMBARDIER.COM FLAGSTAR.COM COLORADO.EDU MIAMI.EDU STANFORD.EDU SHELL.COM

PNCPA.COM NIPRO.COM FOODLAND.COM AUROBINDO.COM UTILITYTRAILER.COM ARCHIVE2

COULSONGROUP.COM COMPASSNRG.COM GENESISNET.COM BPATPA.COM SUNSETHCS.COM

BLUEBONNETNUTRITION.COM BRPRINTERS.COM EMPIRICAL-RESEARCH.COM STRATISVISUALS.COM

BOLTONUSA.COM ABSOLUTERESULTS.COM SSMSJUSTICE.COM TONLYELE.COM SMARTERASP.NET

NATUS.COM QUANTUMGROUP.COM SLIMSTOCK.COM MCH-GROUP.COM EDAN.COM

SWIRESPO.COM MUSCHERT-GIERSE.DE MTMRECOGNITION.COM ENPRECIS.COM

DUTTONFIRM.COM JCWHITE.COM JBINSTANTLAWN.NET CAPCARPET.COM ALEXIM.COM

DRC-LAW.COM DRIVEANDSHINE.COM ALTERNATIVETECHS.COM OAKDELL.COM

ATTENTION!!!

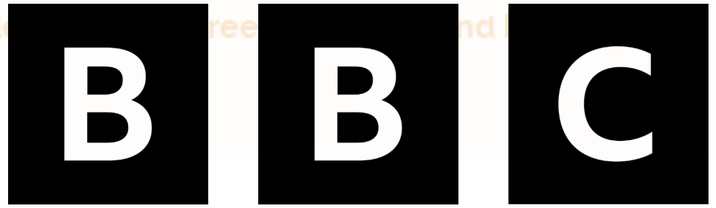
We have never attacked hospitals, orphanages, nursing homes, charitable foundations, and we will not.

Commercial pharmaceutical organizations are not eligible for this list;

they are the only ones who benefit from the current pandemic.

If an attack mistakenly occurs on one of the foreg… provide the d… free … nd …

vulnerabilities.



All old emails do not work, below is a new email for communication

E-mail: unlock@… …m…t.com

OR

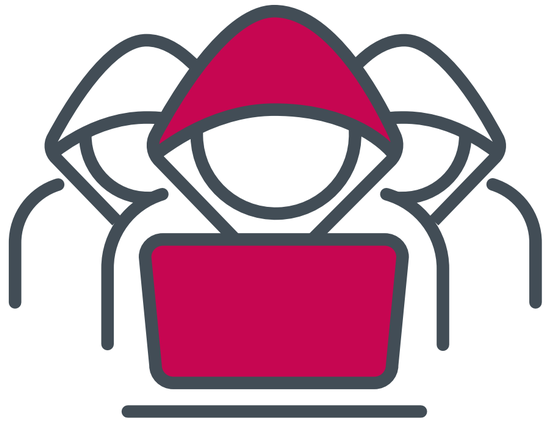
E-mail: unlock@rsv-box.com

If you are interested in detailed logs and files of any companies, we have - write to us

±2700 organizácií

91 miliónov jednotlivcov

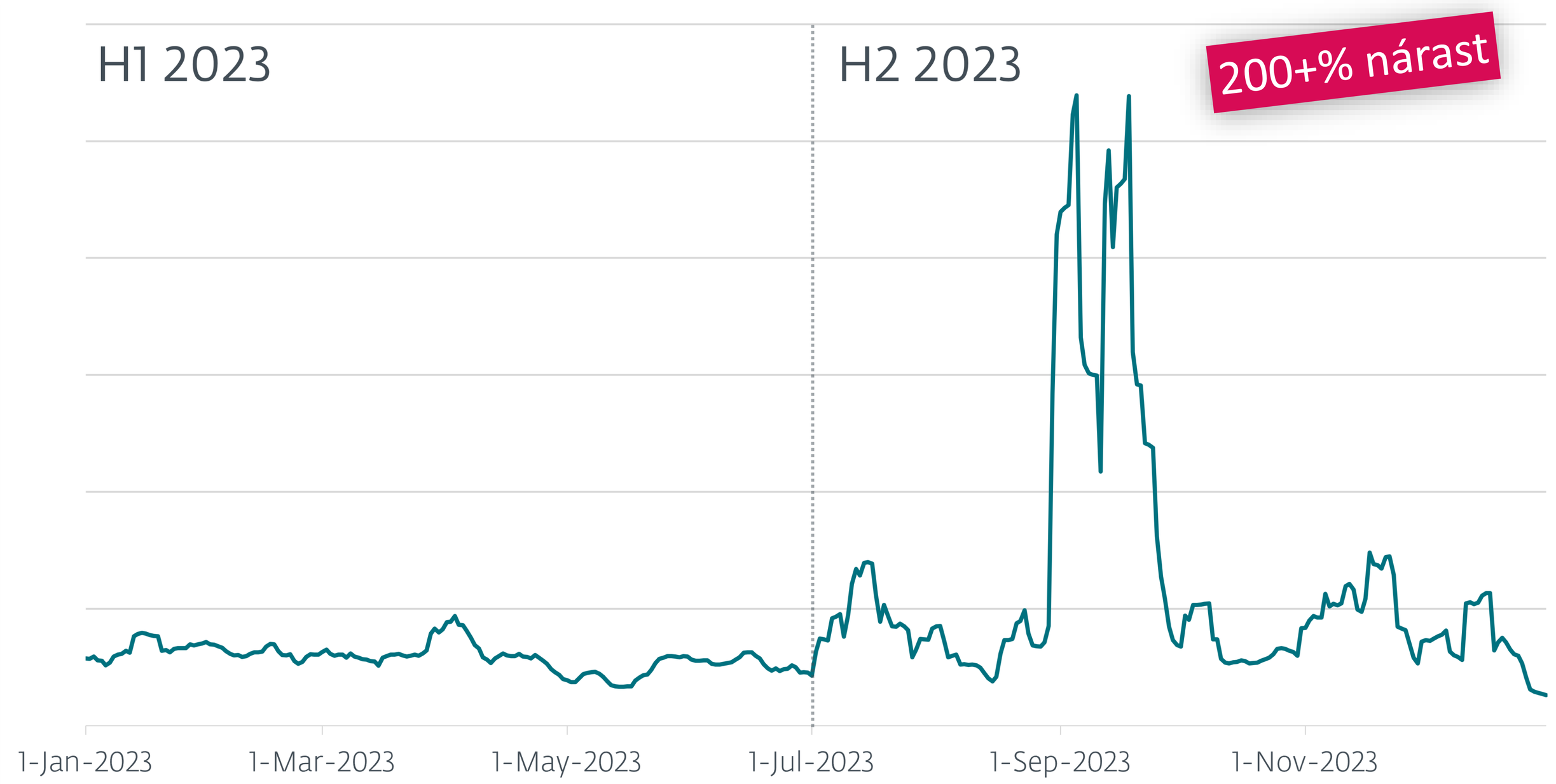
Najdrahší kyberútok?

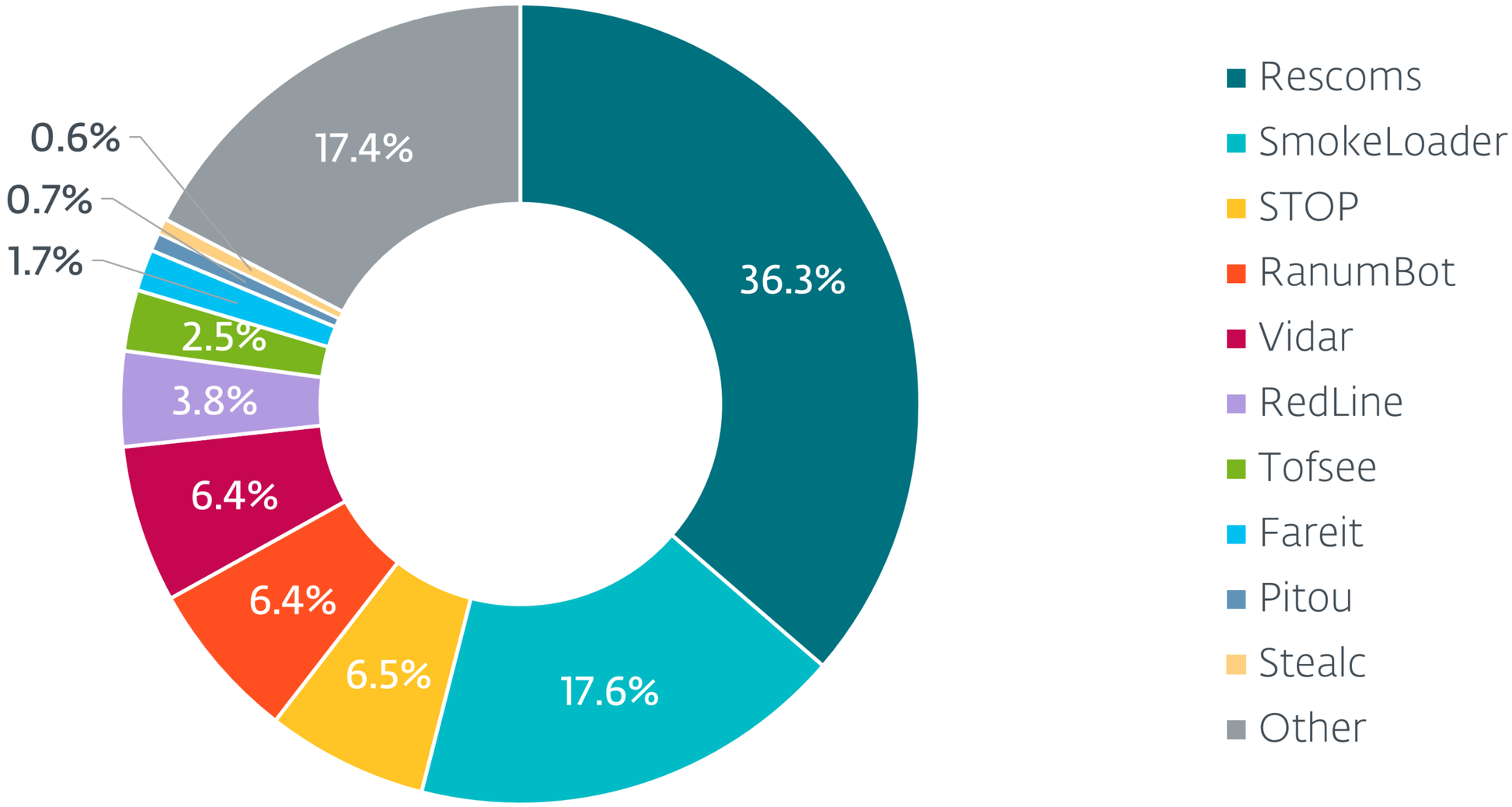


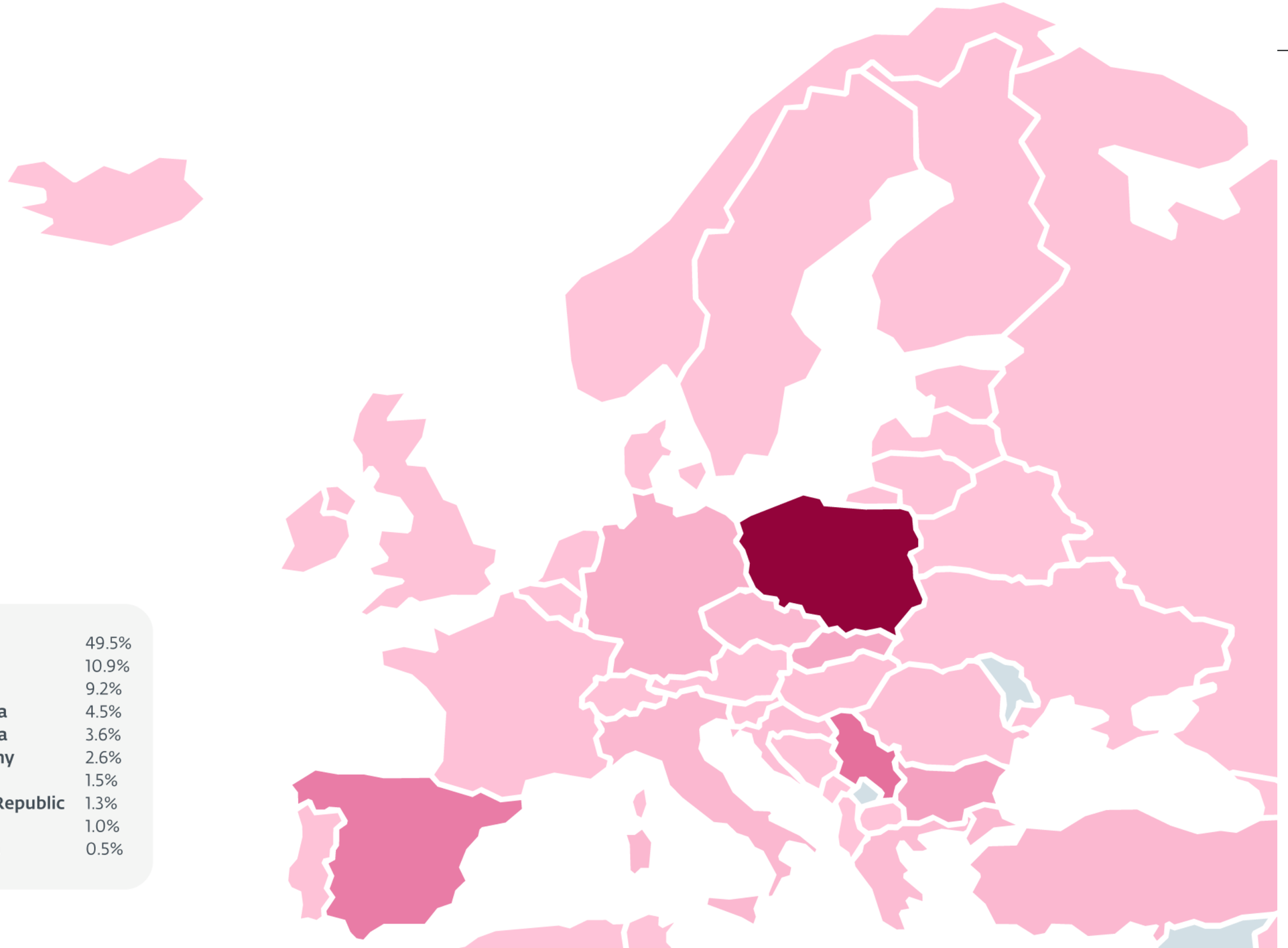
“zárobok”:
USD 75-100 miliónov

škody:
USD 14 miliárd

AceCryptor & Rescoms


H1 2023
H2 2023
200+% nárast
1-Jan-2023
1-Mar-2023
1-May-2023
1-Jul-2023
1-Sep-2023
1-Nov-2023


36.3%
17.6%
6.5%
6.4%
6.4%
3.8%
2.5%
1.7%
0.7%
0.6%
17.4%
Rescoms
SmokeLoader
STOP
RanumBot
Vidar
RedLine
Tofsee
Fareit
Pitou
Stealc
Other



Poland	49.5%
Serbia	10.9%
Spain	9.2%
Bulgaria	4.5%
Slovakia	3.6%
Germany	2.6%
Italy	1.5%
Czech Republic	1.3%
Greece	1.0%
Croatia	0.5%

Szanowny Panie,

Jestem Sylwester [redacted] z [redacted].
Waszą firmę polecił nam partner biznesowy.
Prosimy o wycenę załączonego wykazu zamówień.
Poinformuj nas również o warunkach płatności

Czekamy na Twoją odpowiedź i dalszą dyskusję.

--

Pozdrawiam

Sylwester [redacted]

+48 [redacted]

www.[redacted].pl

Godziny otwarcia:
pn-pt: 8.00-17.00, **sb:** 8.00-12.00

Ochrona danych osobowych - obowiązek informacyjny RODO

Uprzejmie informujemy, że Państwa dane osobowe znajdują się w bazie danych Klientów [redacted] Sylwester (Administrator danych) i są przetwarzane w celu realizacji współpracy handlowej, wykonania umowy sprzedaży, utrzymania relacji biznesowych. Państwa dane osobowe nie są wykorzystywane do profilowania Państwa lub do zautomatyzowanego podejmowania decyzji względem Państwa oraz nie są przekazywane do państw trzecich. Państwa dane osobowe będą przetwarzane przez administratora danych przez okres niezbędny dla realizacji prawnie uzasadnionych interesów administratora danych. Posiadają Państwo prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu i prawo wniesienia skargi do organu nadzorczego.
Więcej informacji na temat przetwarzania Państwa danych oraz na temat praw, które Państwu w związku z tym przysługują znajdziecie Państwo na naszej stronie internetowej w zakładce "Prywatność":
https://[redacted]

Добро утро

Във връзка с телефонния ни разговор, молим за оферта за списъка с артикули в прикачения файл

Благодаря ти

Hristina Dimitrova
Export Manager

DEVOREX PLC
Member of the Gamrat S.A.

Zone Chiirite
4109 Branipol
Plovdiv Regio
T: +359 32 6
M: +359 884
E: h_dimitro
W: www.dev

Dobrý deň,

Zašlite nám prosím ponuku podľa zoznamu v priloženom súbore.

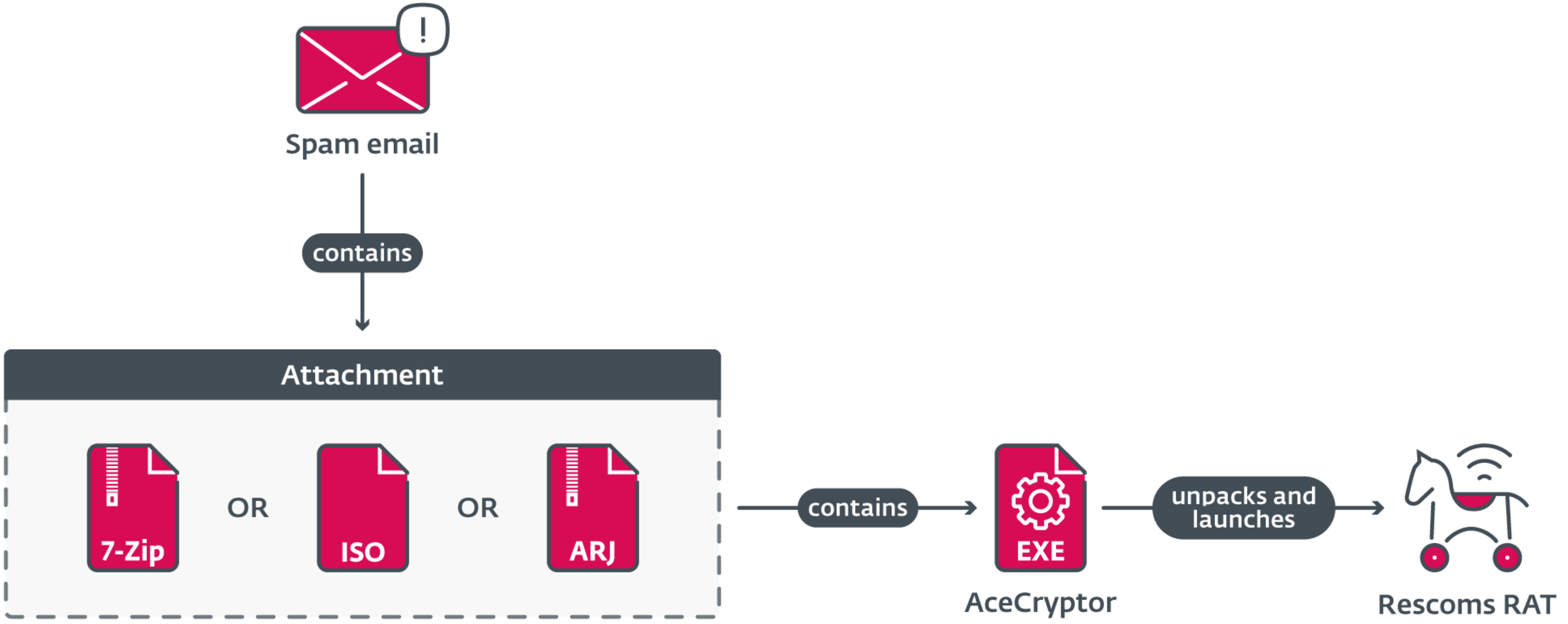
Uveďte prosím presný čas dodania.

Ďakujem.

S pozdravom

Michaela Jančová

tel.: 0337782424 fax: 0337782424

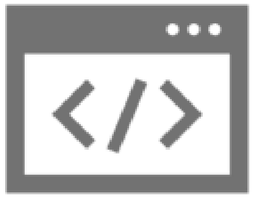

Spam email
contains
Attachment
7-Zip
OR
ISO
OR
ARJ
contains
EXE
AceCryptor
unpacks and launches
Rescoms RAT

Telekopye

Telekopye

Telekopye

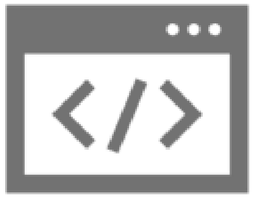
Telekopye



Generovanie obsahu

Web, Email, SMS

Telekopye



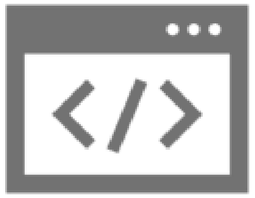
Generovanie obsahu

Web, Email, SMS

Telegram bot

Technologie

Telekopye



Generovanie obsahu

Web, Email, SMS

Telegram bot

Technologie

Kopye - kopija

Spearphishing

Telekopye

Telekopye

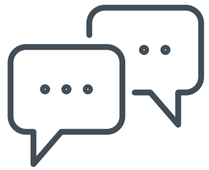
Komunita

Podpora

Telekopye

Komunita

Podpora



Zdieľanie

Rady, tipy, skúsenosti

Telekopye

Komunita

Podpora

Zdieľanie

Rady, tipy, skúsenosti

Návody

Manuály, blogy

Telekopye

Komunita

Podpora

Zdieľanie

Rady, tipy, skúsenosti

Návody

Manuály, blogy

Poplatky

Spoločný účet

Vyberte si z **2 070 606** nabídek

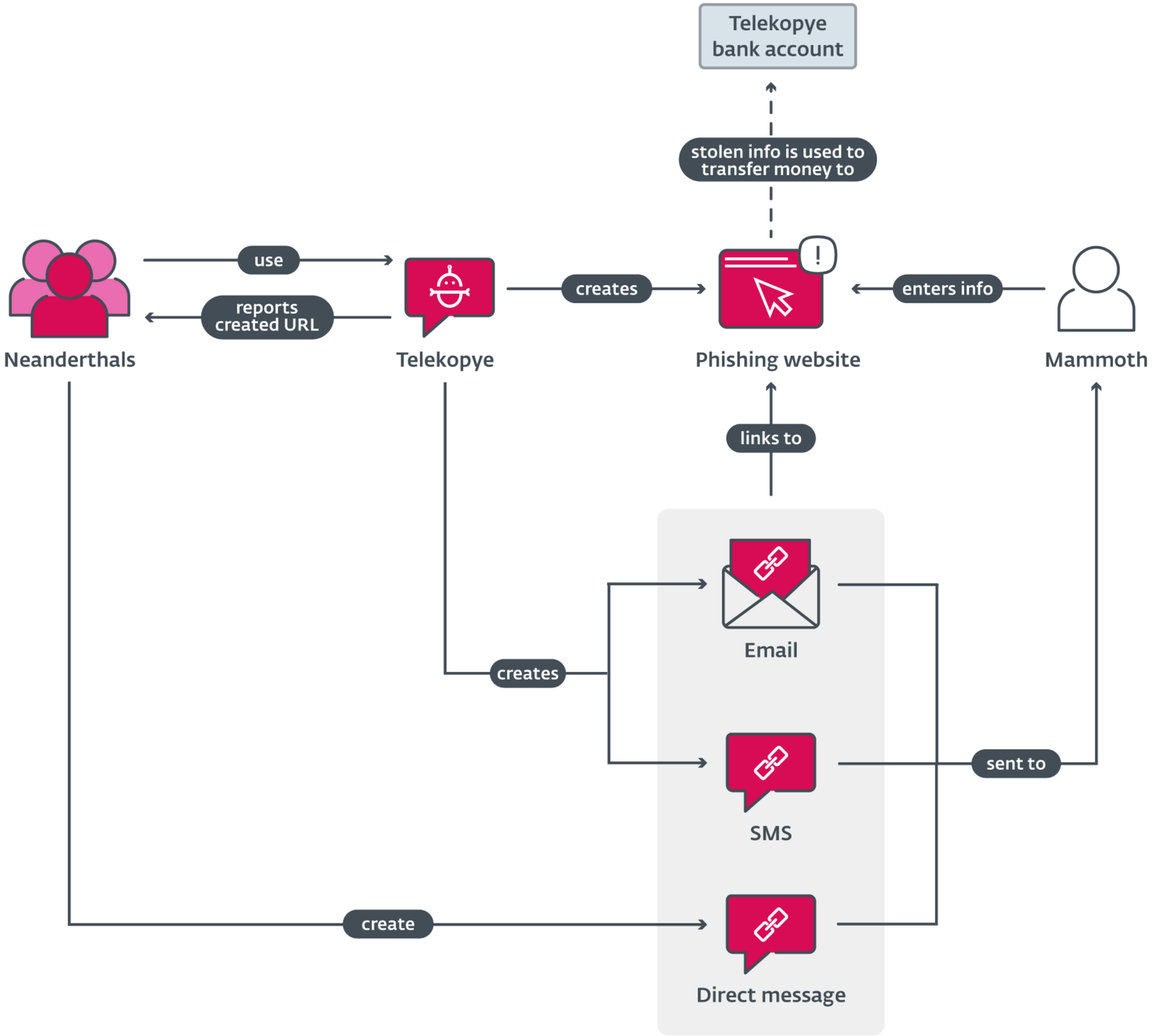
Inzeráty celkem: **1548927**, inzerce za 24 hodin: **57200**

Přivítali jsme zákazníka s pořadovým číslem **4 000 000**.

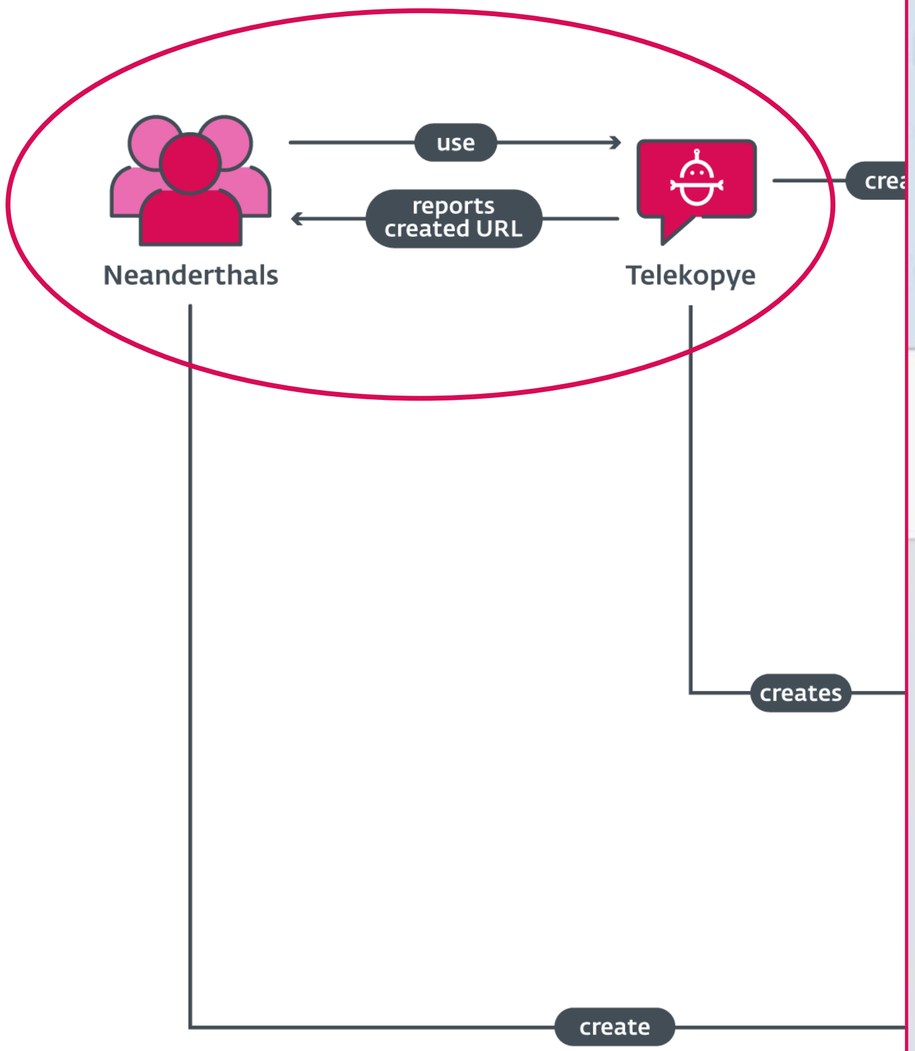
Mamuti?

МАМОНТ СЛИЛСЯ


YOU GET A SPEAR!
YOU GET A SPEAR!
YOU GET A SPEAR!
EVERYONE GETS A SPEAR!


Telekopye bank account
stolen info is used to transfer money to
use
reports created URL
creates
enters info
Neanderthals
Telekopye
Phishing website
Mammoth
links to
Email
creates
SMS
sent to
create
Direct message

TELEKOPYE

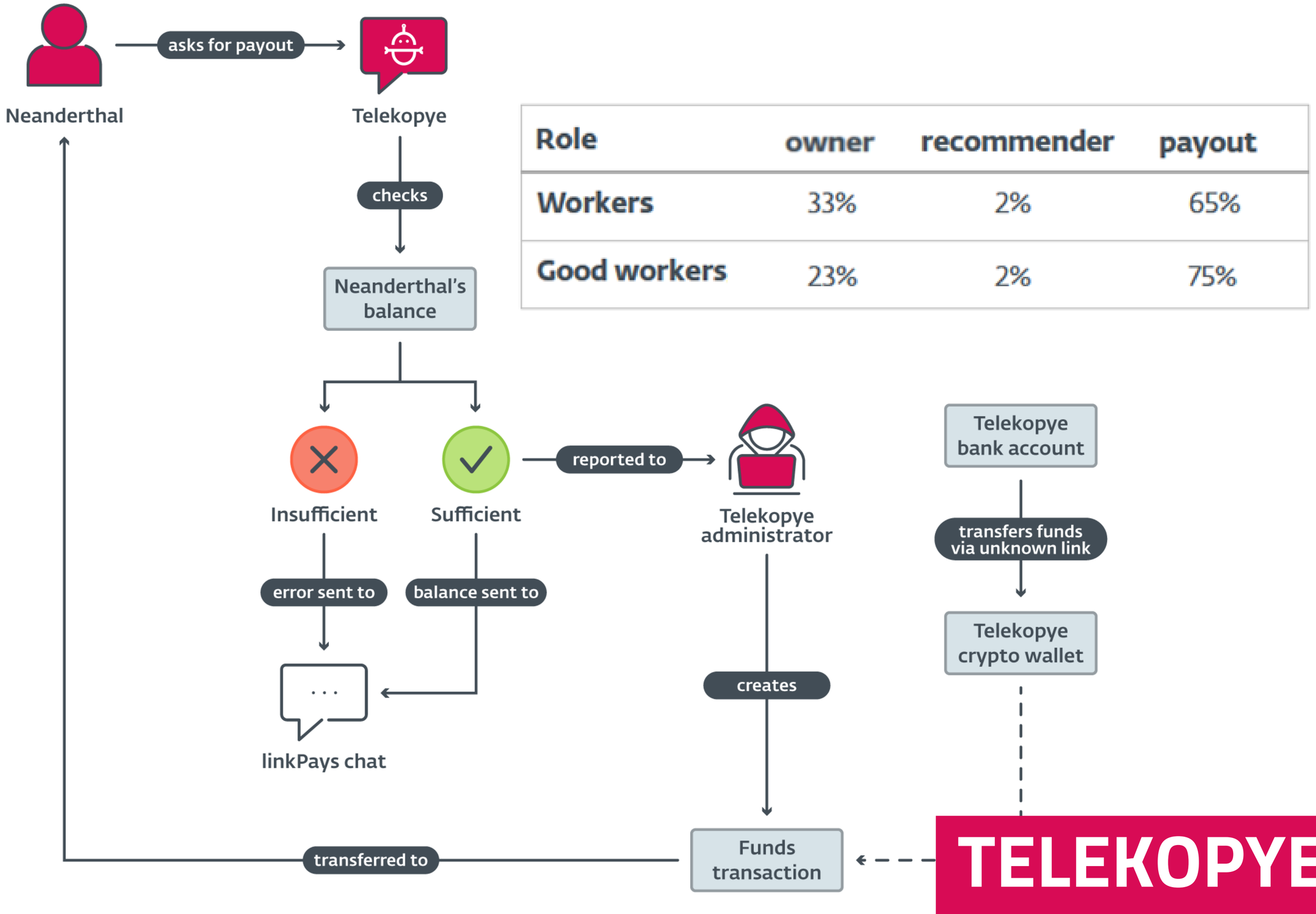


Меню создания ссылок: 22:11
[Link creation menu]

Словакия [Slovakia]
Испания [Spain]
Швецария [Switzerland]
Чехия [Czech Republic]
Румыния [Romania]
Болгария [Bulgaria]
Польша [Poland]
Германия [Germany]
Австралия [Australia]
Англия [England]
Италия [Italy]
BlaBlaCar
Назад [Back]

Выберите сервис: 22:11
[Selected service]
Ebay
Назад [Back]

TELEKOPYE



Role	owner	recommender	payout
Workers	33%	2%	65%
Good workers	23%	2%	75%

Kategórie mamutov

- Nováčik
- Bežný používateľ
- Nezáujem
- Debil
- Obchod / predajňa

Kategórie mamutov

- Nováčik
- Bežný používateľ
- Nezáujem
- Debil
- Obchod / predajňa

“... taký človek má 100 a viac aktívnych a 500 dokončených inzerátov, predal všetko čo sa dá (a predal by i svoju matku), ...”

ebay

The receipt of funds

Buyer

FCS	%namef%
Product	%title%
Address	%address%

Receive %amount2% EUR

The buyer has already paid for the order, it remains only to receive the money and transfer the goods.

The order is paid

%title%

Product	%amount2% EUR
Total	**%amount2% EUR**

Zásilkovna.cz

Doklad o zaplaceni od zakaznika

500 CZK

Dětská postylka

Vaše zbozi bylo propustěno!

Kupujicí již za objednávku zaplatil.

Details about dodani

Dodaci address

Vážní 521, 503 41 Hradec Králové

Prijmeni

Vera Nemcova

Po obdržení hotovosti odešlete zboží zákazníkovi. podle zadaných údajů nebo převést zboží kurýrovi, který vám zavolá do 12 hodin.

Uveďte kupujícího po dodání zboží číslo podání! Zboží musí být dodáno do do 3 dnů od obdržení finančních prostředků

500 CZK

ZÍSKAT PENÍZE

Platba je bezpecna

Kliknutím na tlačítko "ZÍSKAT PENÍZE" souhlasíte s tím. Podminky používání online - služba "Bezpečná nabídka"

ČNB ČESKÁ NÁRODNÍ BANKA

Přihlaste se do systému

Zadejte klientské číslo

Datum narození

Zadejte heslo

Přihlášení do Klientského portálu je zabezpečeno prostřednictvím SSL.

Pokračovat

mBank

Rodné číslo s lomítkem nebo cestovní pas sé

Zadajte sve zákaznické číslo nebo se přihláše

Datum narození

Zadejte své heslo

PIN aplikace

PIN prohlížeče

Zadejte příjmení matky za svobodna

Zadejte rodne prijmeni matky s diakritikou

Pokračovat

BANKA CREDITAS

Přihlaste se do online bankovnictví

Přihlašovací jméno

Datum narození

Zadejte heslo

Všechna připojení jsou šifrována end-to-end

Další

ESET RESEARCH

Telekopye: Hunting Mammoths using Telegram bot

Analysis of Telegram bot that helps cybercriminals scam people on online marketplaces

Radek Jizba

24 Aug 2023 • 18 min. read

More and more people nowadays prefer to buy goods online. And why not? It's convenient, goods will be delivered to your doorstep, and if you choose one of many online marketplaces, it's even possible to save some money. Sadly, scammers abuse this, targeting these services and their customers for the scammer's benefit. They can create a listing for goods they don't own or don't

Similar Articles

ESET RESEARCH
New Telegram-abusing Android RAT discovered in the wild

ESET RESEARCH
Not-so-private messaging: Trojanized WhatsApp and Telegram apps go after cryptocurrency wallets

ESET RESEARCH
LATAM financial cybercrime: Competitors-in-crime sharing TTPs

welivesecurity BY ESET | Award-winning news, views, and insight from the ESET security community | Englis

TIPS & ADVICE | BUSINESS SECURITY | ESET RESEARCH | FEATURED | TOPICS | ABOUT US

ESET RESEARCH

Telekopye: Chamber of Neanderthals' secrets

Insight into groups operating Telekopye bots that scam people in online marketplaces

Radek Jizba

23 Nov 2023 • 16 min. read

We recently published a blogpost about Telekopye, a Telegram bot that helps cybercriminals scam people in online marketplaces. Telekopye can craft phishing websites, emails, SMS messages, and more.

In the first part, we wrote about technical details of Telekopye and hinted at

Similar Articles

ESET RESEARCH
Telekopye: Hunting Mammoths using Telegram bot

ESET RESEARCH
Scarabs colon-izing vulnerable servers

ESET RESEARCH
New Telegram-abusing Android RAT discovered in the wild

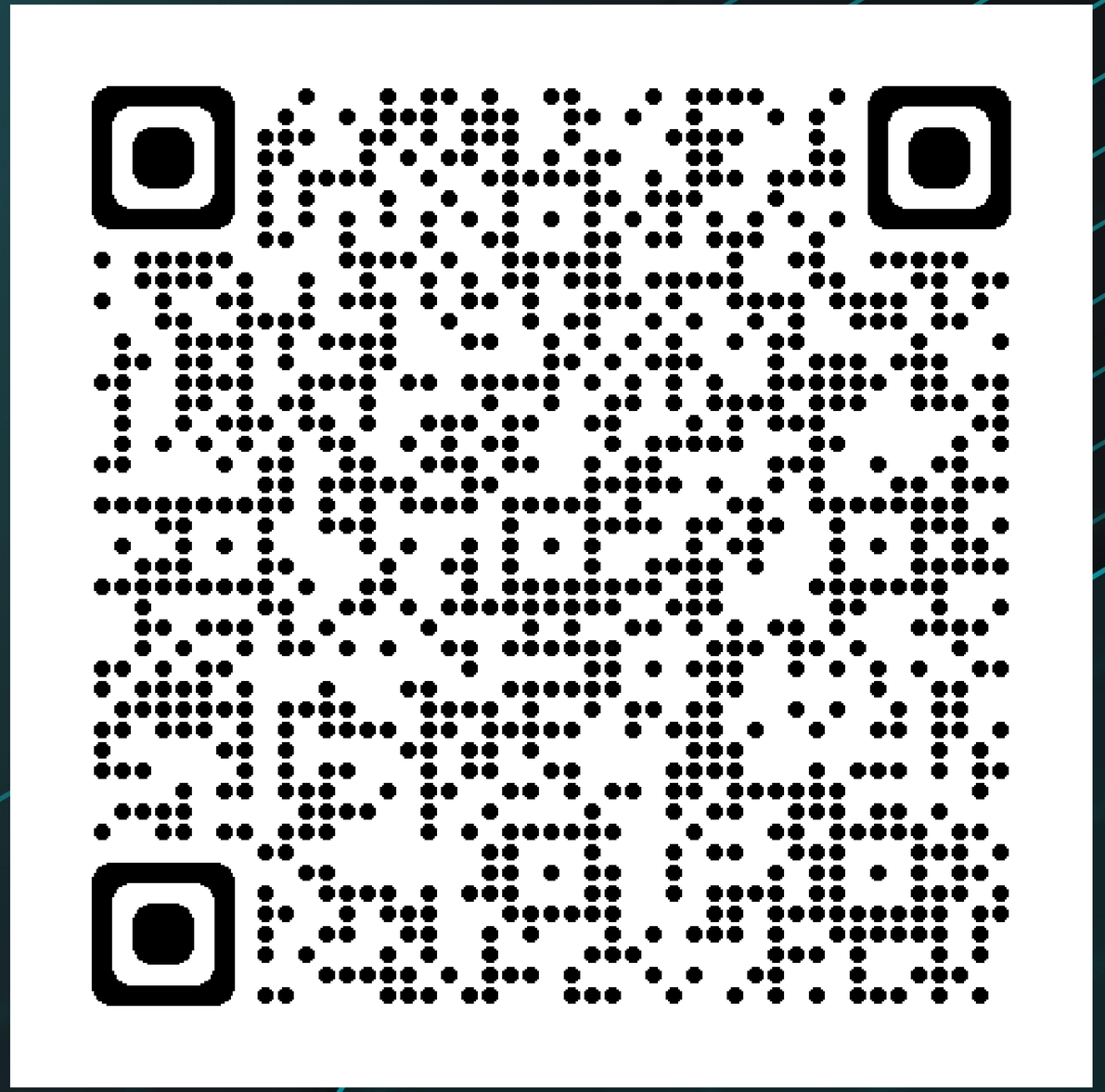
Digital Security
Progress. Protected.

Threat Report

H2 2023

June-November

(eset):research



SECURITY DAYS

Ďakujem

@Robert_Lipovsky @Rockouter

Digital Security
Progress. Protected.

& SME KONFERENCIE