

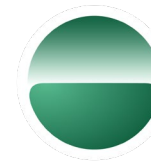


12TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

TITLE SPONSOR



Island

EYES WIDE OPEN



CYBER SECURITY SUMMIT
Security solutions through collaboration.™

12th Annual Cyber Security Summit | October 24-26, 2022

cybersecuritysummit.org

“Armchair Cyberwarriors”

The First 100 Days of Cybercriminal and
Hacktivist Activities Related to the
Russian War in Ukraine

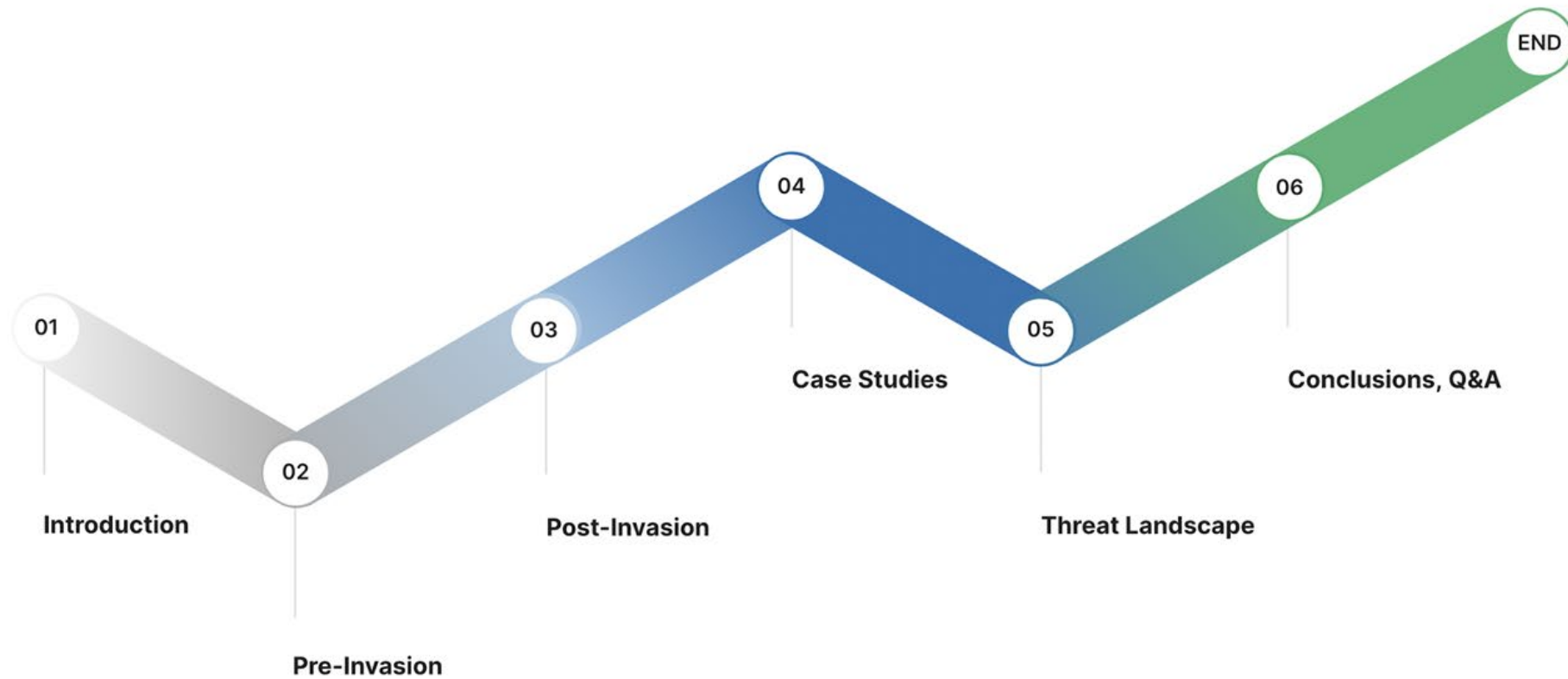
·||· Recorded Future®

Biography

- **Alexander Leslie**
- Associate Threat Intelligence Analyst, Advanced Cybercrime & Engagements (ACE) @ **Recorded Future**
- Research includes Russian & Russian-speaking threat actors.



Recorded Future®



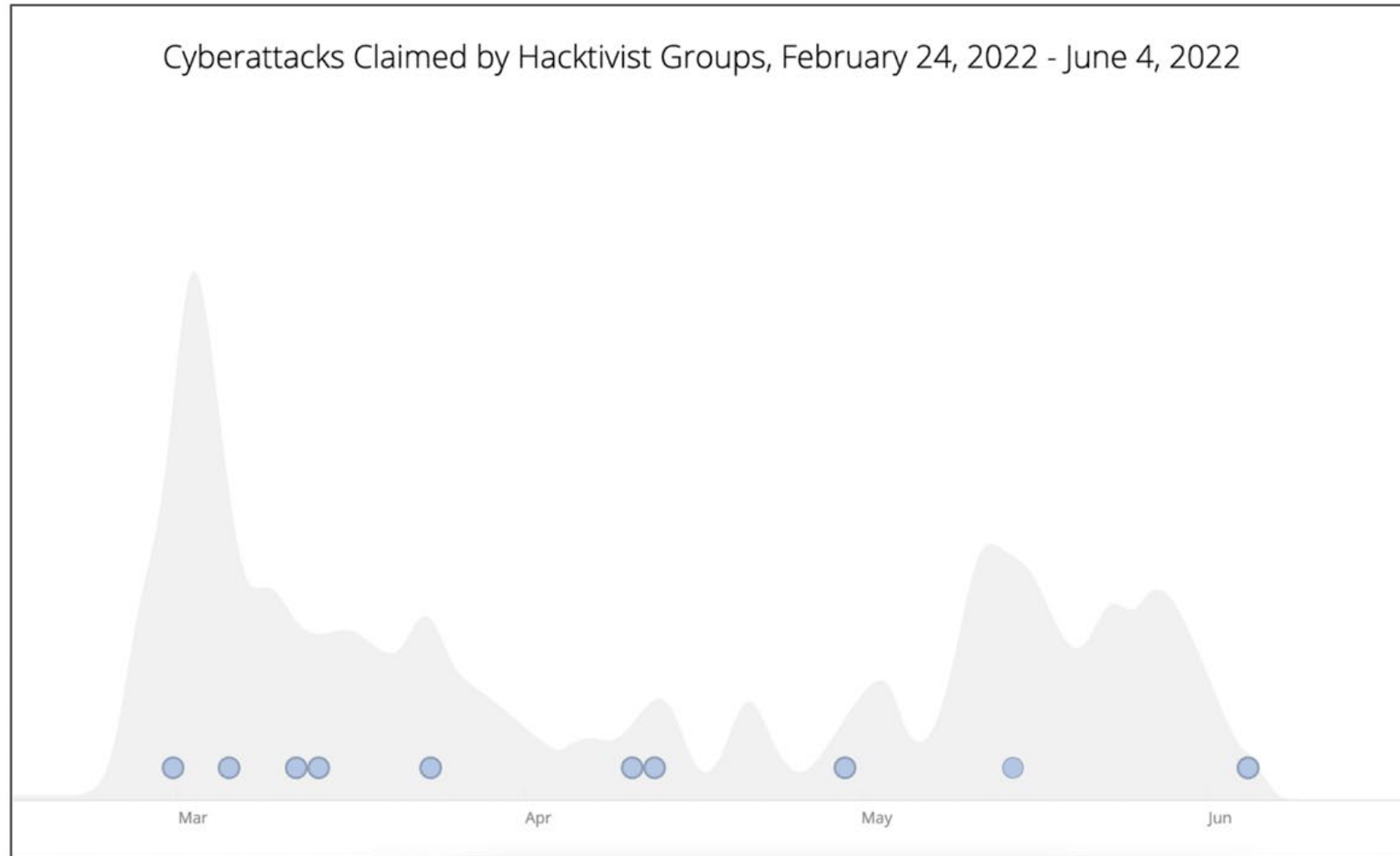
PRESENTATION MAP

Recorded Future®

Introduction



Research Questions



**700,000
References**

**Avg. 100,000
References per
Month**

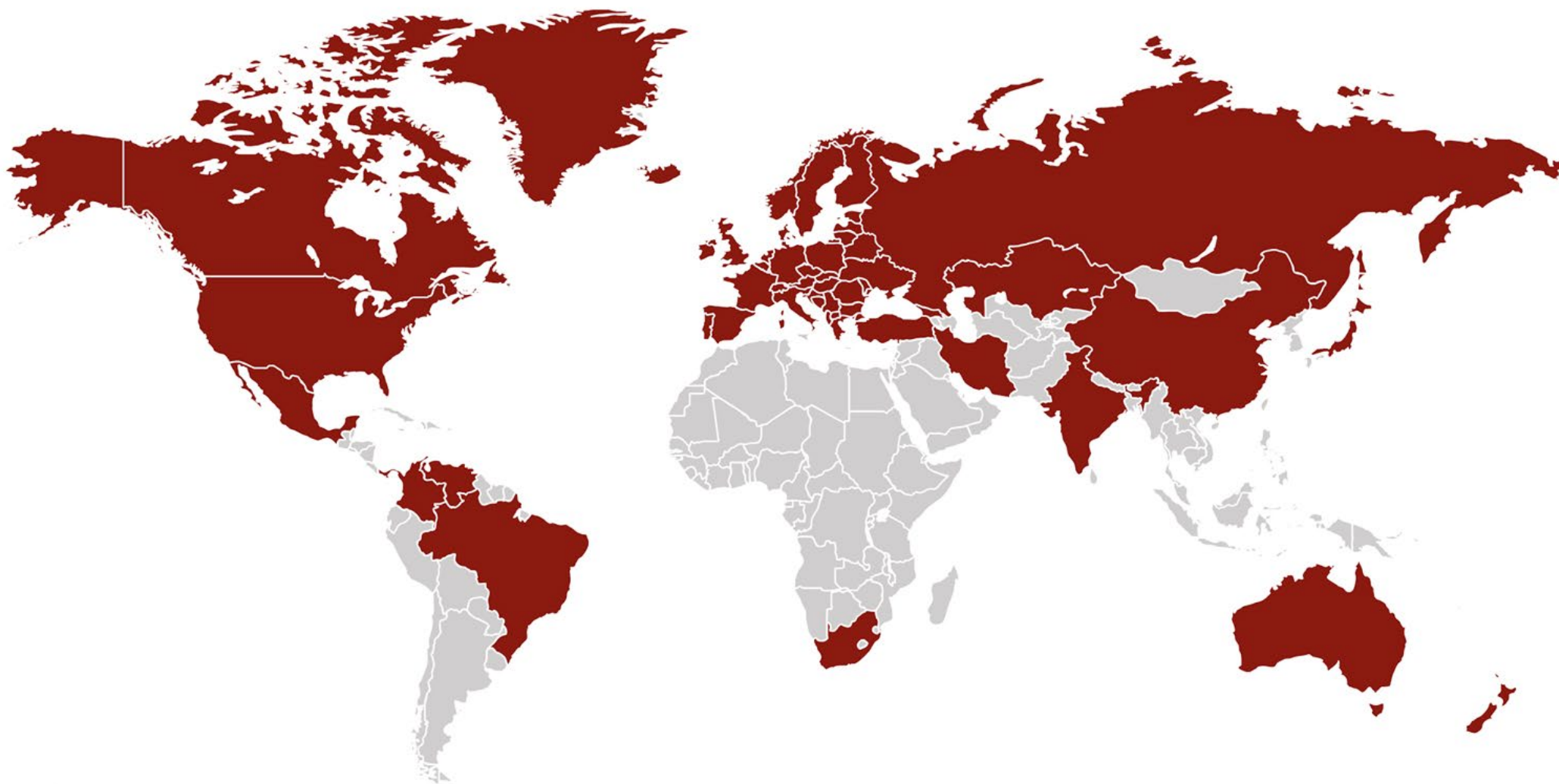
**250+ Threat
Actor Groups**

500+ Victims

75+ Countries

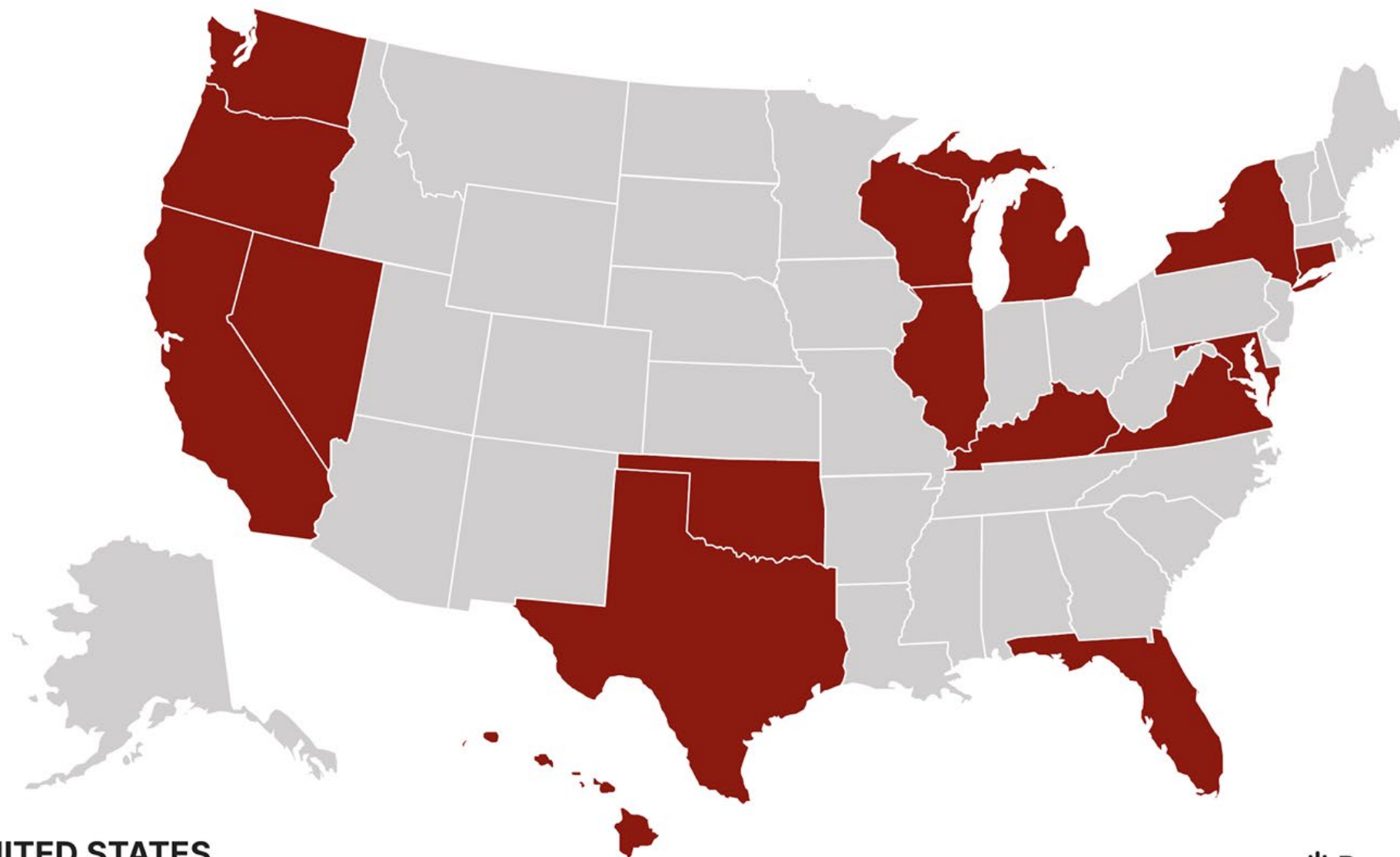
\$3.7T ARR

Recorded Future®



WORLD

Recorded Future®



UNITED STATES

Recorded Future®



RUSSIA

Recorded Future®

Research Questions

- What explains the observed rise in unique references to cyberattacks perpetrated by **politically motivated TAs** following February 24, 2022? Which groups claim responsibility for the **most** attacks? Which groups claim responsibility for attacks that result in the most **impact**? What are their **tools, TTPs, and IOCs**?
- How has the Russian war in Ukraine **changed** the hacktivist and cybercriminal threat landscapes? What **lessons** can be learned about the first 100 days of the war and how can we **apply** those lessons to future geopolitical crises.
- What is the **risk** to governments, enterprises, employees, partners, and clients? What steps can we take to **mitigate** risk and potential impact?

Methodology



Pre-Invasion (September 29, 2021 - February 23, 2022)

 Recorded Future®

Ilya Sachkov Arrest

(Sept. 29, 2021)

**Russia detains cyber-security tycoon
Ilya Sachkov in treason case**

🕒 29 September 2021

**Moscow Court Rejects Release Request Of
Cybersecurity Company Chief Arrested On
Treason Charge**

**Moscow Court Extends Pretrial Detention Of Cybersecurity Company
Chief Charged With Treason**



Recorded Future®

“REvil” Arrests

(January 14, 2022)

Moscow court arrests all REvil ransomware hackers detained after FBI request to Russia

All the eight individuals are suspected of committing a crime stipulated under Part 2 of Article 187 of Russia’s Criminal Code

MOSCOW, January 15. /TASS/. Moscow’s Tverskoy Court has ruled to keep in custody all eight members of the REvil hacking group responsible for ransomware attacks, who were earlier apprehended by the Russian Federal Security Service (FSB) following the US request, the court’s press service told TASS on Saturday.



Recorded Future®

Infraud Organization Arrests

(January 22, 2022)

Thirty-six Defendants Indicted for Alleged Roles in Transnational Criminal Organization Responsible for More than \$530 Million in Losses from Cybercrimes

Law Enforcement Dismantles Forum Used to Victimize Millions in all 50 States and Worldwide in One of the Largest Cyberfraud Enterprises Ever Prosecuted by the Department of Justice

Founder of The Infraud Organization
hacking group arrested in Moscow —
source

Three other purported hackers are under a house arrest

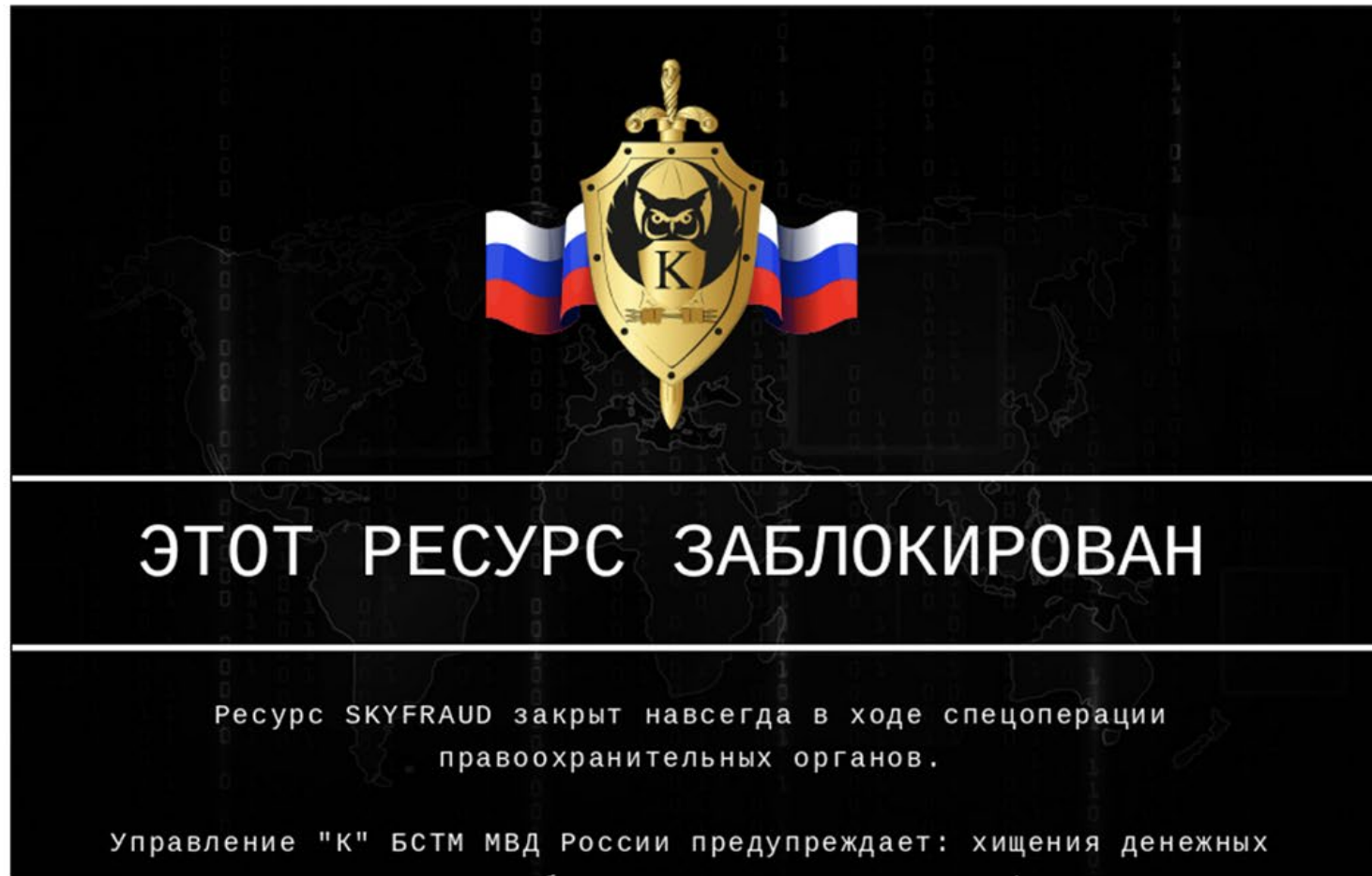
The screenshot shows a dark-themed web interface for a marketplace. At the top is a navigation bar with icons for HOME, BUY, BILLING, ORDERS, SUPPORT, SETTINGS, and EXIT. Below this is a sub-navigation bar with links for CW, Fullz, Dumps, and My Cart. The main section is titled 'Search dumps' and contains a search form with the following fields: Price (with a plus sign), Basename (dropdown), Card type (dropdown), Level (dropdown), and Ctype (dropdown). Below these are fields for BINs, Bankname, Country, SVC, and Additional. There are checkboxes for 'Fresh only (+1\$)', 'With T1 Orig', and 'Discount dumps'. A 'Search' button is on the right. Below the search form is a 'Search result:' section with a table of results.

BIN	Type	Code	EXP	Country	Bank	Price	
408625	PLATINUM CREDIT VISA	201	02/14	TURKEYKEY	DENIZBANK AS	65.00\$	<input type="checkbox"/>
408625	PLATINUM CREDIT VISA	201	02/14	TURKEYKEY	DENIZBANK AS	65.00\$	<input type="checkbox"/>

Recorded Future®

Website Seizures

(February 7, 2022)

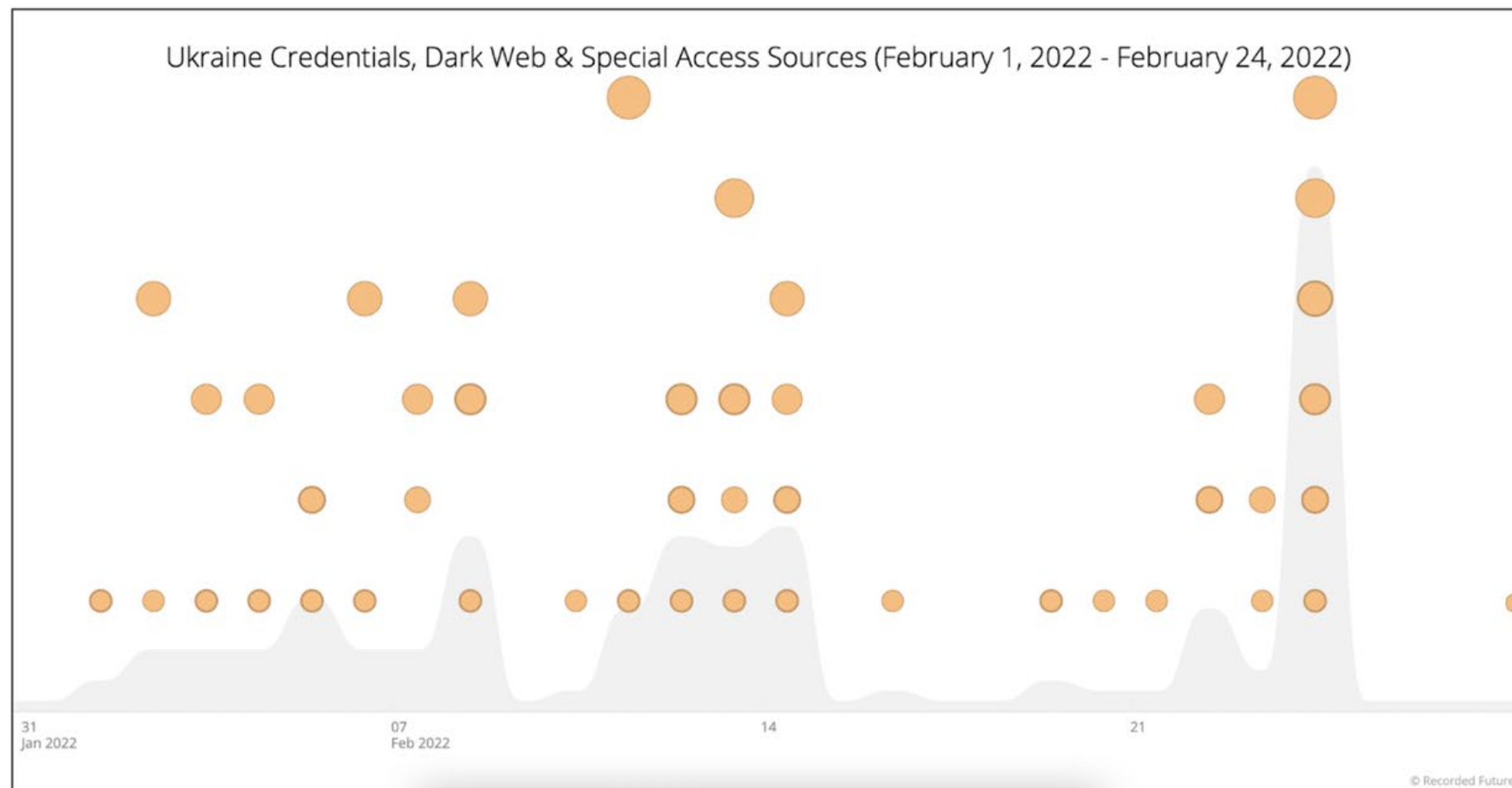


- SkyFraud
- Trump's Dumps
- UAS Shop
- Ferum Shop

Recorded Future®

Credential Leaks

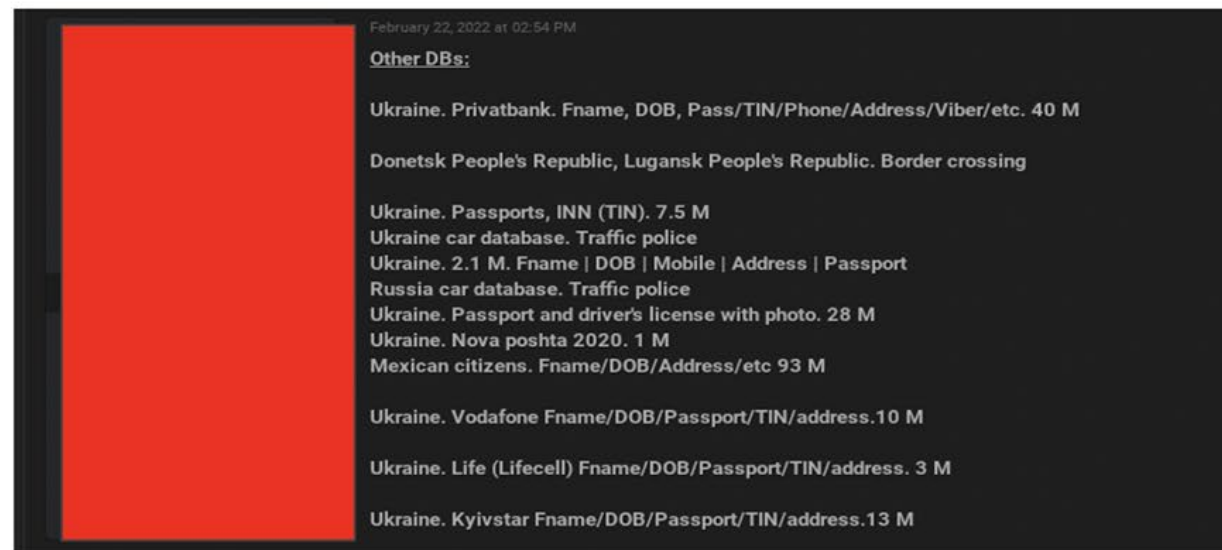
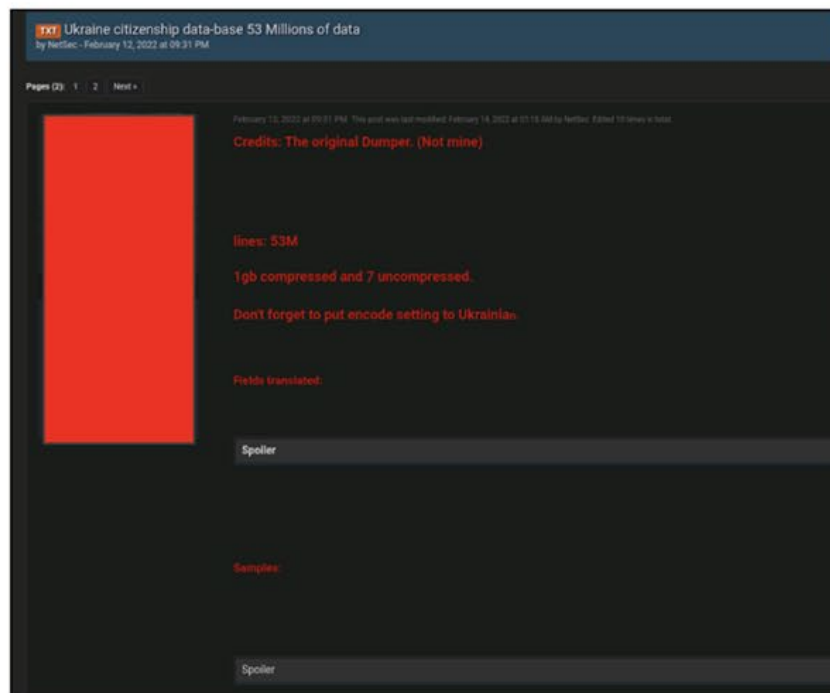
(February 1, 2022 - February 24, 2022)



Recorded Future®

Database Leaks

(February 12, 2022 - February 24, 2022)



Recorded Future®

FreeCivilian Leaks

(February 23, 2022 - February 24, 2022)



About

I sell a database of personal data of citizens of Ukraine.
There is data from several government departments.

News

- > ***NEW*** New leaks
- > ***NEW*** Database statement - diia.gov.ua
- > Deleting a post on RaidForum

Leaks

+ diia.gov.ua - 765 GB ***NEW***
+ e-driver.hsc.gov.ua - 431 GB SOLD
+ wanted.mvs.gov.ua - 3.29 GB
+ minregion.gov.ua - 904 GB
+ health.mia - 96.7 GB
+ mtsbu.ua - OVER 3 TB
motorsich.com
+ kyivcity.com
bdr.mvs.gov.ua
gkh.in.ua
kmu.gov.ua
mon.gov.ua
minagro.gov.ua
mfa.gov.ua
To be continued ...

Recorded Future®

The First 100 Days (February 24, 2022 - June 4, 2022)

Recorded Future®

Formation of Hacktivist Groups & Alliances

(February 25, 2022 - Ongoing)



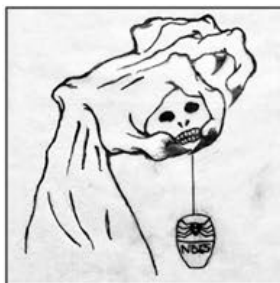
Recorded Future®

Anonymous



Recorded Future®

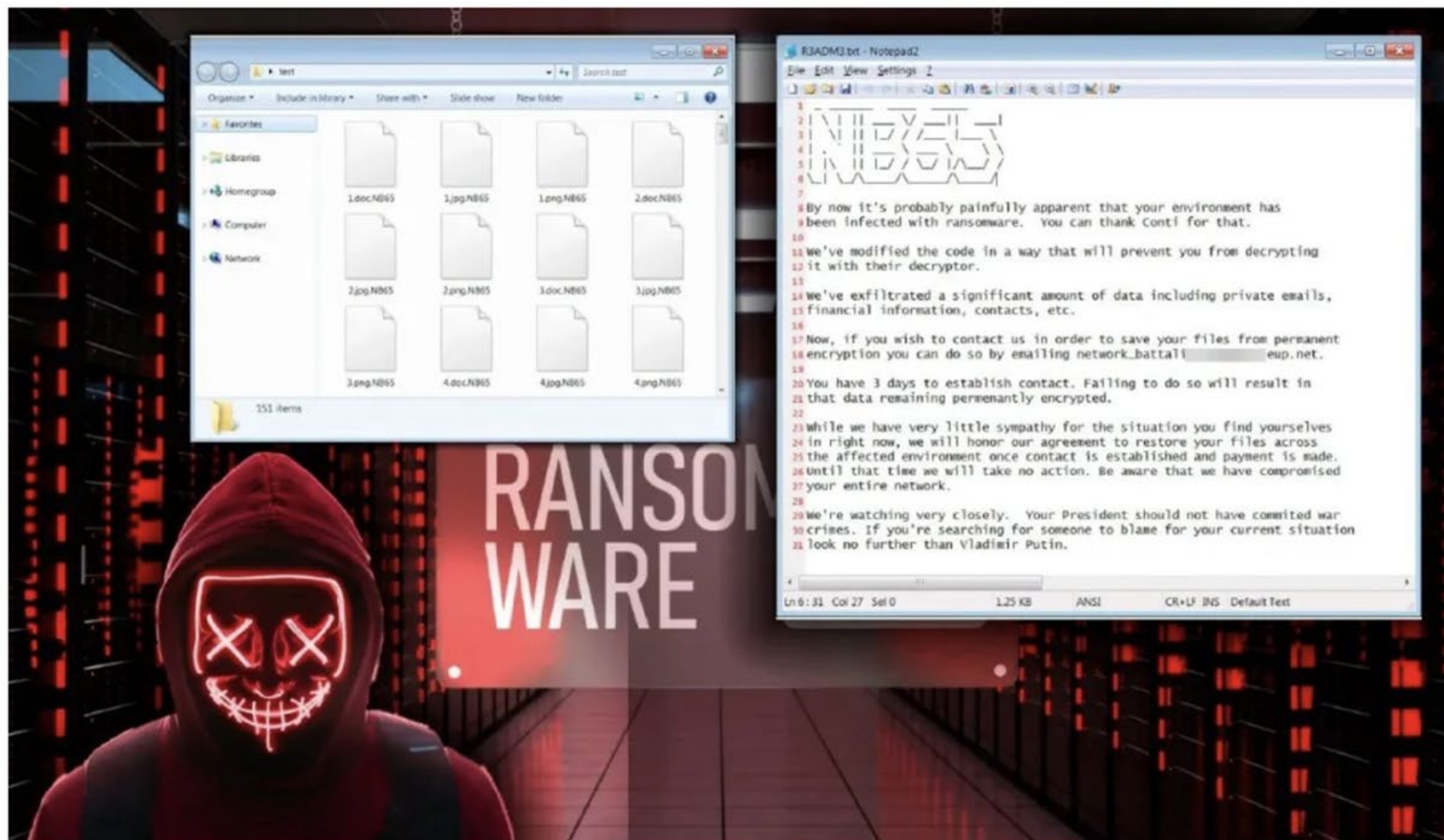
#OpRussia



...and many more.

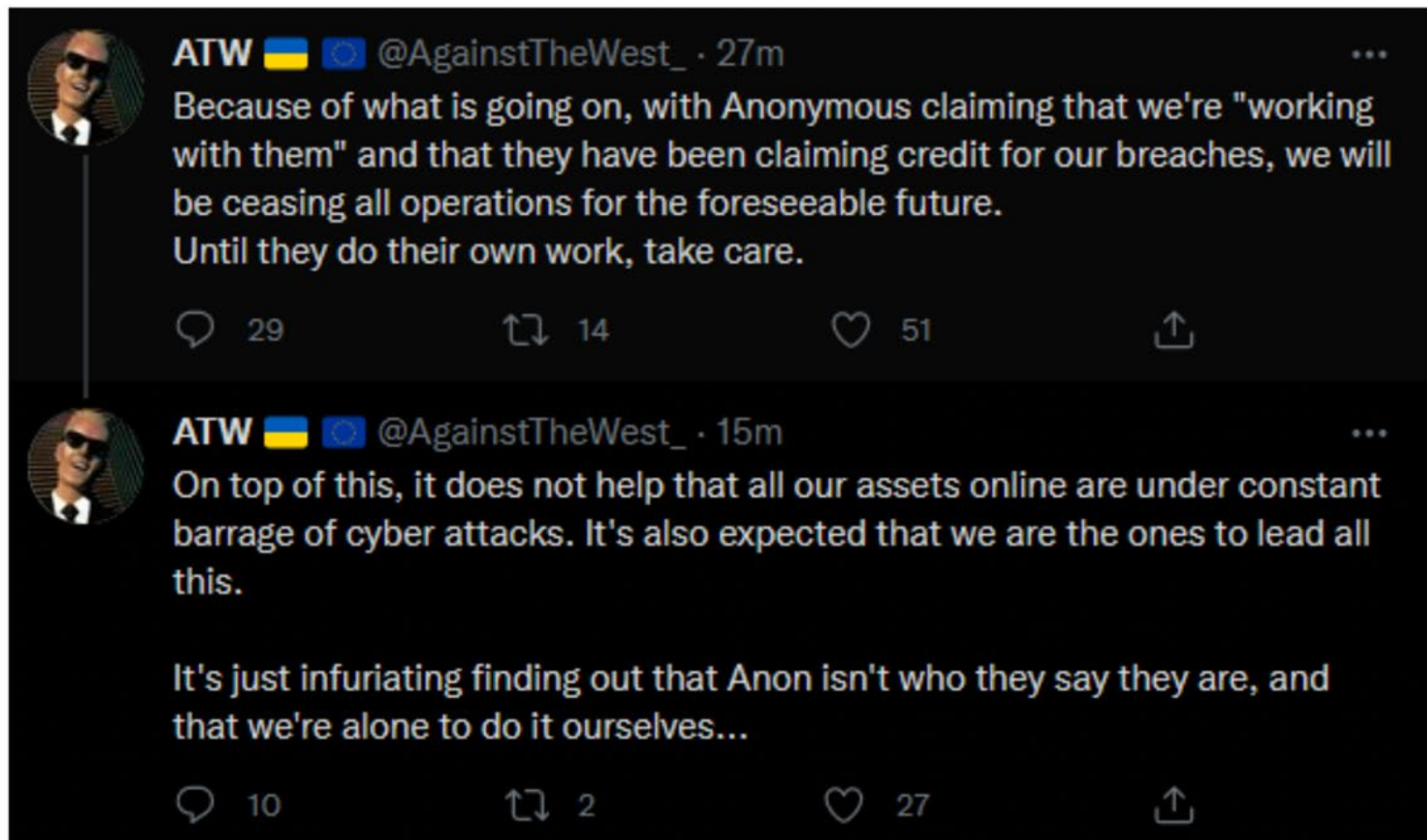
Recorded Future®

Network Battalion 65 (NB65)



Recorded Future®

AgainstTheWest (BlueHornet, APT49, etc.)



Recorded Future®

IT Army of Ukraine



IT ARMY of Ukraine

Вчорашні цілі були успішно відправлені в аут!
Дякуємо усім хто долучився до атаки!
Сьогодні атакуємо сервіси онлайн телебачення.

We knocked off our targets yesterday!
Huge thanks to everyone who joined the attack! Today we'll switch to online TV streaming services.

<https://more.tv/>
<https://osiris.preprod.more.tv/>
https://rendertron.preprod.more.tv
https://gitlab-exporter.preprod.more.tv
https://dagon.preprod.more.tv
94.140.201.116 (80/tcp, 123/udp, 443/tcp, 443/https)
<https://static.more.tv/>
94.140.200.247 (80/tcp, 111/udp, 123/udp, 443/tcp)
94.140.201.247 (80/tcp, 443/tcp)
94.140.201.50 (80/tcp, 443/tcp)
<https://moretv-sport.preprod.more.tv/>
<https://billing-api-test.preprod.more.tv/>
94.140.201.116 (80/http, 443/https)
<https://rc.more.tv/home>
<https://rc.more.tv/api/v1/method.callAnon/login>
94.140.201.135 (80/tcp, 123/udp, 443/tcp)

<https://okko.tv>
185.169.155.118 (80/tcp, 443/tcp)
<https://cabinet.okko.tv/login>
151.236.80.51 (443/https, 443/tcp)



IT ARMY of Ukraine

Ви попрацювали на славу! 🙌
Росіяни відчували сьогодні регулярні перебої в роботі сервісів онлайн телебачення. Продовжуємо тематику вихідного дня, наступна ціль — сервіси замовлення їжі онлайн.
Дякуємо всім за крутий результат!

Great job today! 🙌
Russians have noticed regular hitches in the work of TV streaming services today. We'll stick to our 'weekend theme'. Our next target is online food delivery services.
Thanks again for the stellar results!

<https://vkusvill.ru/>
178.248.232.221 (80/tcp, 443/tcp)
<https://av.ru/>
46.235.185.176 (80/tcp, 443/tcp)
212.193.157.110 (80/tcp, 443/tcp)
46.235.189.110 (80/tcp, 443/tcp)
37.220.163.2 (80/tcp, 443/tcp)
<https://www.okeydostavka.ru/msk>
178.248.237.112 (80/tcp, 443/tcp)
<https://www.delivery-club.ru/moscow>
5.61.236.234 (80/tcp, 443/tcp)
<https://samokat.ru/>
46.235.188.221 (80/tcp, 443/tcp)
46.235.186.103 (80/tcp, 443/tcp)
212.193.155.174 (80/tcp, 443/tcp)
46.235.191.53 (80/tcp, 443/tcp)
37.220.160.159 (80/tcp, 443/tcp)
93.93.88.47 (80/tcp, 443/tcp)

Recorded Future®

Liberator



Recorded Future®

Killnet

KILLNET

CZECHIA APOCALYPSE

☠ Судный день - Чехия

- ☠ Министерство обороны
⚡ <https://mocr.army.cz/>
💎 <https://check-host.net/check-report/8eb6c76kab>
- ☠ Государственная дума
⚡ <https://portal.gov.cz/>
💎 <https://check-host.net/check-report/8eb7060k17>
- ☠ Железнодорожные перевозки
✅ <https://www.cd.cz/>
💎 <https://check-host.net/check-report/8eb768bkf9>
- ☠ Коммерческий Банк
✅ <https://www.kb.cz/>
💎 <https://check-host.net/check-report/8eb79e7k757>

KILLNET

STOP ARMS TRANSFERS

⚠ STOP

- 🔥 Ночная Бомбардировка
- 🛑 STOP ARMS TRANSFERS

1). Международный аэропорт им. Игнация Яна
⚡ <http://plb.pl/>
💎 <https://check-host.net/check-report/8e4f344k122>

Targets on map:

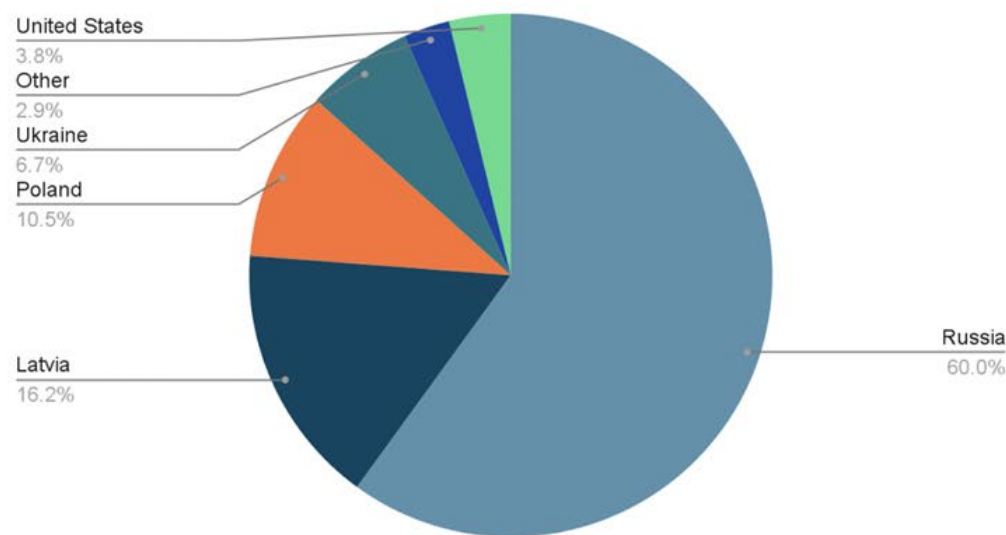
- Щецин SZZ - 0,36 mln
- Былгош BZG - 0,34 mln
- Варшава-Модлин - 0,90 mln
- Варшава Окенце - 9,59 mln
- Вроцлав WRO - 2,00 mln
- Катовице KTW - 2,55 mln
- Краков KRK - 3,44 mln
- Жешув RZE - 0,86 mln
- Люблин LUZ - 5 371
- Даньск GDN - 2,90 mln
- ИЕГ - 12 276 Зелена Гур

Recorded Future®

Key Findings

- Russian individuals and entities constitute approximately **60%** of all claimed cyberattacks. (n=300)
- Distributed denial-of-service (DDoS) accounts for **94%** of all attacks. Website defacement accounts for **3%**.
- IT Army of Ukraine claims responsibility for most targets at approximately **750**. Of these 750, **only ~150 can be verified**.

Attacks by Country



Recorded Future®


Key Findings

- Primary industries targeted include the Russian financial sector (**26%**), Russian government services (**12%**), and Russian critical infrastructure (**7%**).
- In the first 100 days, **85%** of all attacks took place between February 25, 2022 and March 25, 2022.
- Of all the groups associated with Anonymous (approximately 30), we were only able to confirm evidence of successful cyberattacks claimed by **4**.

Changes to the Cybercriminal Threat Landscape

·||· Recorded Future®

Malware-as-a-Service (MaaS)



raccoonstealer
RAID array

User

registration : 01.04.2019
Messages : 75
Reactions : 20

Today at 13:38

New Topic author #132

Dear Clients, unfortunately, due to the "special operation", we will have to close our project Raccoon Stealer
The members of our team who were responsible for critical moments in the operation of the product are no longer with us. 😞
We are disappointed to close our project, further stable operation of the stiller is physically impossible
What will happen to the logs?
Logs can still be downloaded, but the multidownload server has already stopped responding
This means that you need to start downloading the logs one by one, starting with the "fattest" ones (download button on the right in the table on each log)
We apologize for such inconvenience, for not being able to continue to please you with our product, as we have been doing for the last 3 years, but we are forced to close the project for an indefinite period
Please understand our loss
I wish everyone patience, and everyone to find \$ 1,000,000 profit
Thank you ❤️, for this experience and time, for every day, unfortunately everything, sooner or later, comes to an end
Peace for everyone
😞

We don't say goodbye forever. We took a break to regroup and continue work on the second version that had already been started.

We have lost a friend and a great developer. But the project has become a part of our life in 3 years, so we decided to continue working. We will rewrite the lost moments and completely new build and panel. In an improved form, rewritten from scratch and optimized.
Expect us in a few months. In the meantime, we're going offline!

















Avoid throwing! WE DO NOT WORK ANY MORE!

🔔 Complaint

👍 Like + Quote ↩ Reply

Recorded Future®

Dark Web Shops

Stealer	Country	Links	Outlook	Info	Struct	Date	Size	Vendor	Price	Action
Redline	 Departamento de Montevideo ISP: Administracion Nacional de Telecomunicaciones	accounts.google.com asuswebstorage.com scgi.ebay.com flowergirlsdressforless.com baxterautoparts.com autoservicio.ute.com.uy autoservicio.ute.com.uy login.adinet.com.uy inia.org.uy grooveshark.com Show more...	-	-	 archive.zip	2022.06.13	0.11Mb	Monsterlog silver	\$ 10.00	Buy
Redline	 Quintana Roo ISP: Total Play Telecomunicaciones SA De CV	es-la.facebook.com admin.jeromitransfers.com.mx play.hbomax.com wrapbootstrap.com bravenet.com super.walmart.com.mx mercadolibre.com abasteo.mx bitso.com blm.com Show more...	-	-	 archive.zip	2022.06.13	1.20Mb	Monsterlog silver	\$ 10.00	Buy
Redline	 Western Province ISP: Dialog Axiata Plc	winwinik.net prepaidcloud.tech bitcoindoubler.store paxful.com vivafaucet.website accounts.coinmarketcap.com clickscoin.com feyorajunkie.com thenext.link app.stash.com Show more...	-	-	 archive.zip	2022.06.13	0.47Mb	Monsterlog silver	\$ 10.00	Buy
Redline	 Uttar Pradesh ISP: World Star Communication	majestyhash.com freebitco.in accounts.google.com m.facebook.com minex.world twilio.com dollarhuge.com hit4hit.org userlytics.com itc1.site Show more...	-	-	 archive.zip	2022.06.13	0.03Mb	Monsterlog silver	\$ 10.00	Buy
Redline	 Tamil Nadu ISP: Hathway IP over Cable Internet Access	portal.medibuddy.in lenskart.com accounts.paytm.com pocket52.com cs-india-support.coinswitch.co opinionbureau.com moneycontrol.com thepanelstation.com udemy.com panelist.cint.com Show more...	-	-	 archive.zip	2022.06.13	0.41Mb	Monsterlog silver	\$ 10.00	Buy
Redline	 Baranya ISP: DiGi Tavkozlesi es Szolgaltato Kft	alza.hu dirtywindows.hu alza.hu estone.cc ittott.tv windowsbox.hu m.facebook.com ittott.tv alinda.hu accounts.paradoxplaza.com Show more...	-	-	 archive.zip	2022.06.11	0.10Mb	Monsterlog silver	\$ 10.00	Buy
Redline	 Departamento de Guatemala ISP: INTERNET TELECOMUNICATION COMPANY DE GUATEMALA, S.A.	hightechgt.com hightechgt.com magix.com mega.nz rye.usac.edu.gt 192.168.0.1 1777.com.gt my.eset.com 192.168.1.1 registro.usac.edu.gt Show more...	-	-	 archive.zip	2022.06.13	1.29Mb	Monsterlog silver	\$ 10.00	Buy
Redline	 England ISP: TalkTalk	giffgaff.com secure.tesco.com reed.co.uk id.avast.com quidco.com lycamobile.co.uk briskoda.net odtoys.com tkmaxx.com burtonpower.com Show more...	-	-	 archive.zip	2022.06.13	0.08Mb	Monsterlog silver	\$ 10.00	Buy

Recorded Future®

Dark Web Shops



Recorded Future®

Dark Web Marketplaces

Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace

Russian Resident Indicted on Conspiracy Charges Related to Operating Hydra Market

The Justice Department announced today the seizure of Hydra Market (Hydra), the world's largest and longest-running darknet market. In 2021, Hydra accounted for an estimated 80% of all darknet market-related cryptocurrency transactions, and since 2015, the marketplace has received approximately \$5.2 billion in cryptocurrency.

The seizure of the Hydra servers and cryptocurrency wallets containing \$25 million worth of bitcoin was made this morning in Germany by the German Federal Criminal Police (the Bundeskriminalamt), in coordination with U.S. law enforcement.

Recorded Future®

Dark Web Marketplaces

THIEF
World

Search... 0 XMR Make a deposit Messages EN COBALTANGO

CATEGORIES all Products The shops **Open shop** TO BUYERS SELLERS GARANT Track my order 1 XMR = 187.66 USD

Home / Big Discounts On Weapons / Javelin ATGM

Javelin ATGM


Weapon

from 30 000 USD / 1pcs




159.86358307578 XMR

Київ

The FGM-148 Javelin is a man-portable, "fire-and-forget" antitank guided missile (ATGM) system with an effective range of 2.5 km. It was designed to defeat heavily armored vehicles such as main battle tanks and lighter-skinned military vehicles. The weapon also has capability against other target types like fortifications, bunkers, and helicopters.

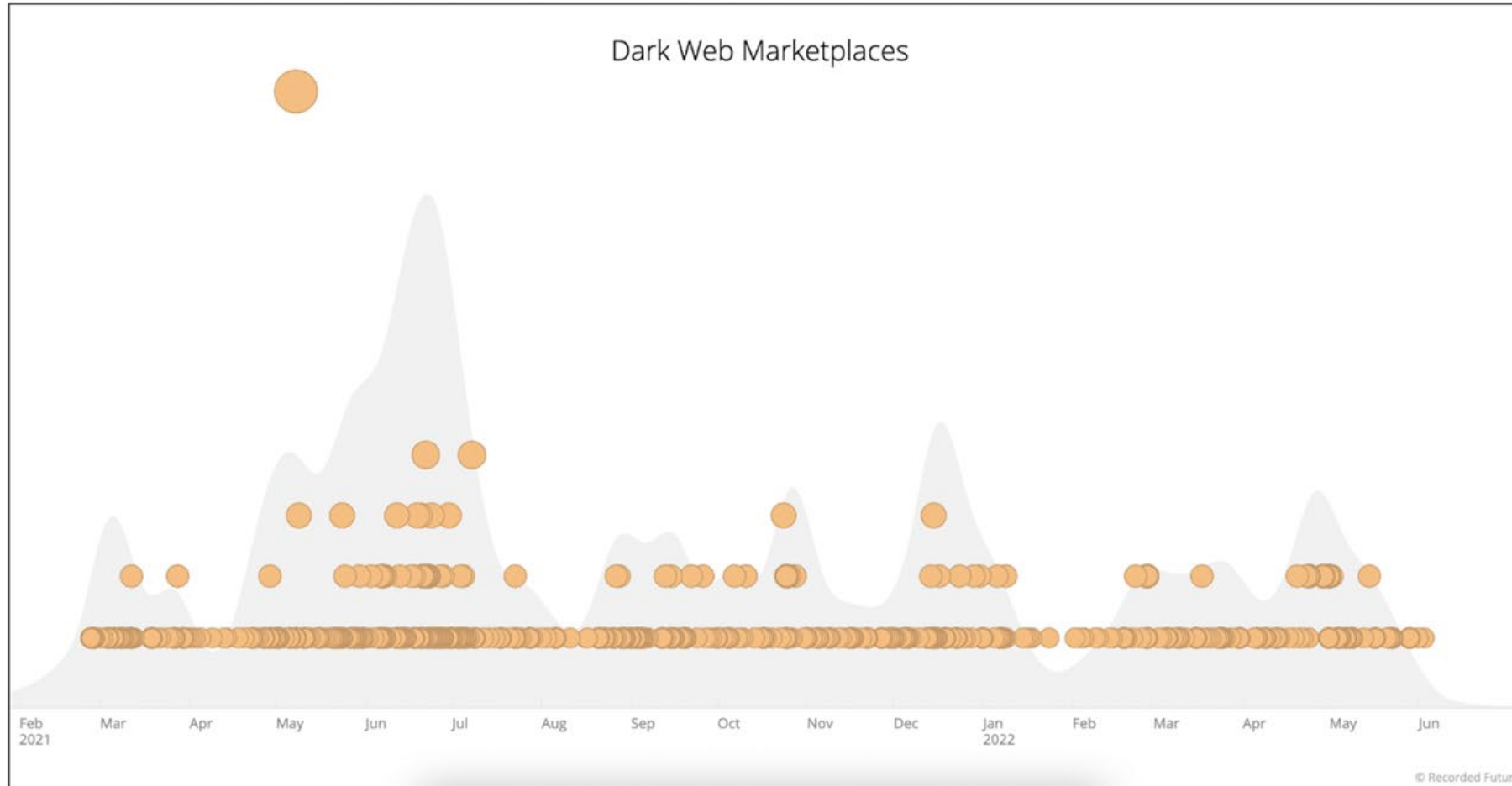


0.0
rating



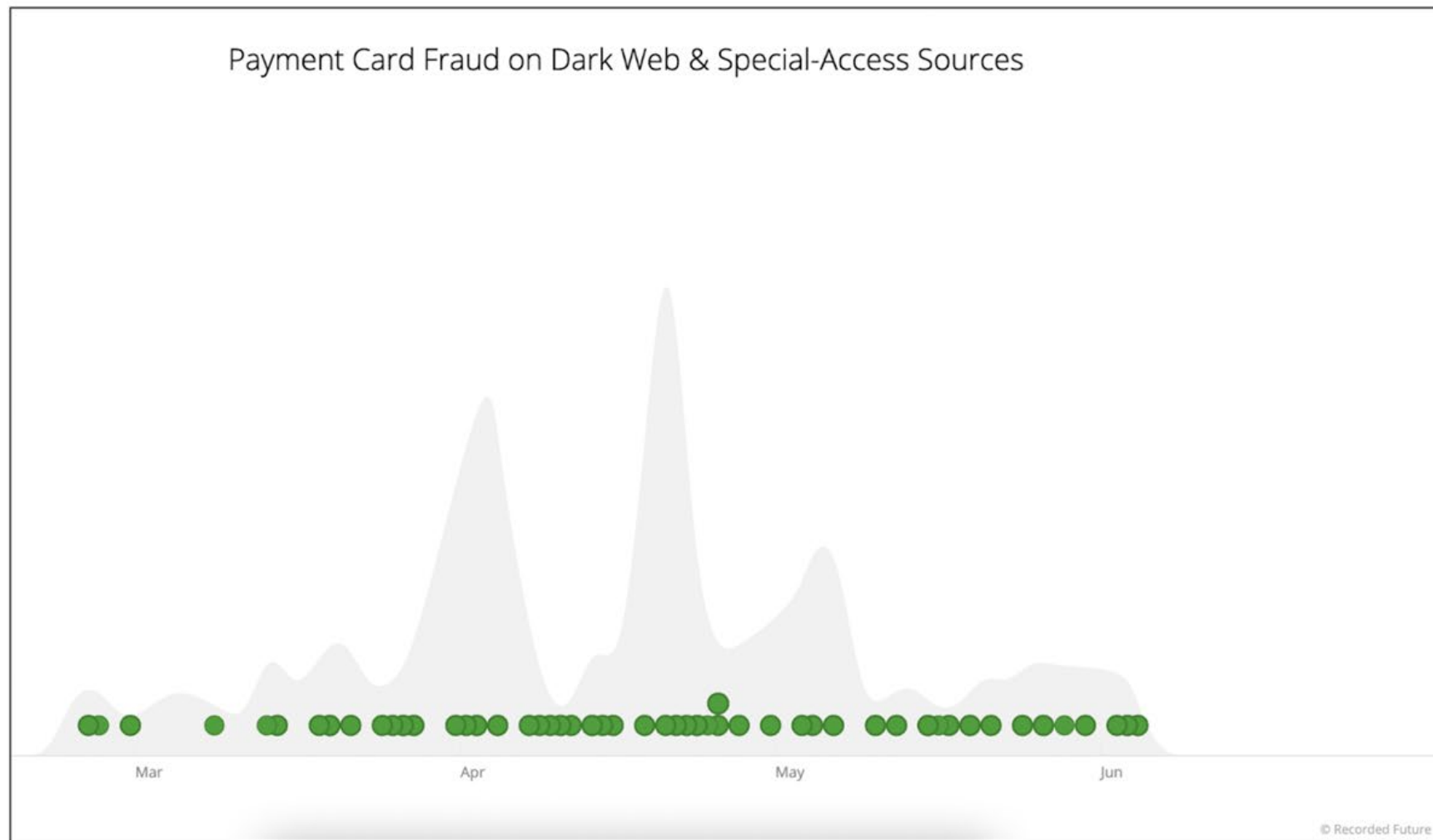
Recorded Future®

Dark Web Marketplaces



Recorded Future®

Payment Card Fraud







Recorded Future®

Ransomware

Многие спрашивают нас, будет ли наше международное сообщество пентестеров с пост оплатой, угрожать западу на критически важные инфраструктуры в ответ на кибер агрессию к России? Наше сообщество состоит из многих национальностей мира, большая часть наших пентестеров — это жители СНГ в том числе русские и украинцы, но также в нашей команде есть американцы, англичане, китайцы, французы, арабы, евреи и многие другие. Наши программисты разработчики проживают на постоянной основе в разных странах мира в Китае, США, Канаде, России и Швейцарии. Наши сервера находятся в Нидерландах и Сейшеллах, все мы простые и миролюбивые люди, все мы Земляне. Для нас это просто бизнес и все мы аполитичны. Нас интересуют только деньги за нашу безобидную и полезную работу. Мы всего лишь проводим платное обучение системных администраторов всего мира, как правильно настроить корпоративную сеть. Мы никогда и ни при каких обстоятельствах не будем принимать участие в кибератаках на критические инфраструктуры любой страны мира и вступать в какие-то международные конфликты.

Many people ask us, will our international community of post-paid pentesters, threaten the west on critical infrastructure in response to cyber aggression against Russia? Our community consists of many nationalities of the world, most of our pentesters are from the CIS including Russians and Ukrainians, but we also have Americans, Englishmen, Chinese, French, Arabs, Jews, and many others in our team. Our programmers developers live permanently around the world in China, the United States, Canada, Russia and Switzerland. Our servers are located in the Netherlands and the Seychelles, we are all simple and peaceful people, we are all Earthlings. For us it is just business and we are all apolitical. We are only interested in money for our harmless and useful work. All we do is provide paid training to system administrators around the world on how to properly set up a corporate network. We will never, under any circumstances, take part in cyber-attacks on critical infrastructures of any country in the world or engage in any international conflicts.

**Support ALPHV**
348845



Support AL...

Мы крайне огорчены происходящим.В нашем бизнесе нет национальностей, вымышленных границ или какой-либо иной причины по которой люди могут убивать

14:00:00

Recorded Future®

Ransomware

“WARNING”

💬 The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we are going to use our all possible resources to strike back at the critical infrastructures of an enemy.

📅 2/25/2022

👁 39

📄 0 [0.00 B]

“WARNING”

💬 As a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing that we will use our full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world. We do not ally with any government and we condemn the ongoing war. However, since the West is known to wage its wars primarily by targeting civilians, we will use our resources in order to strike back if the well being and safety of peaceful citizens will be at stake due to American cyber aggression.

📅 2/25/2022

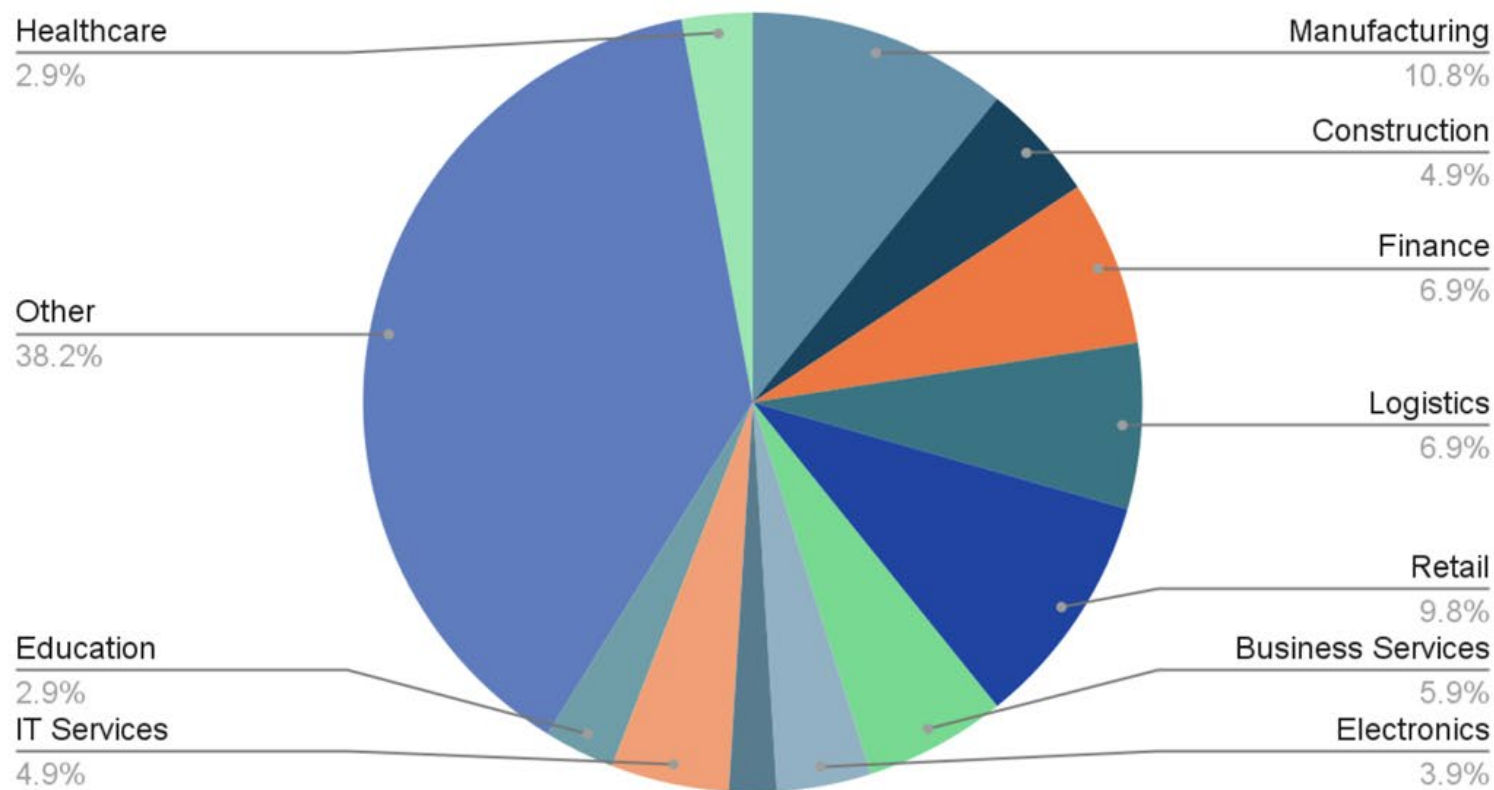
👁 905

📄 0 [0.00 B]

Recorded Future®

Ransomware

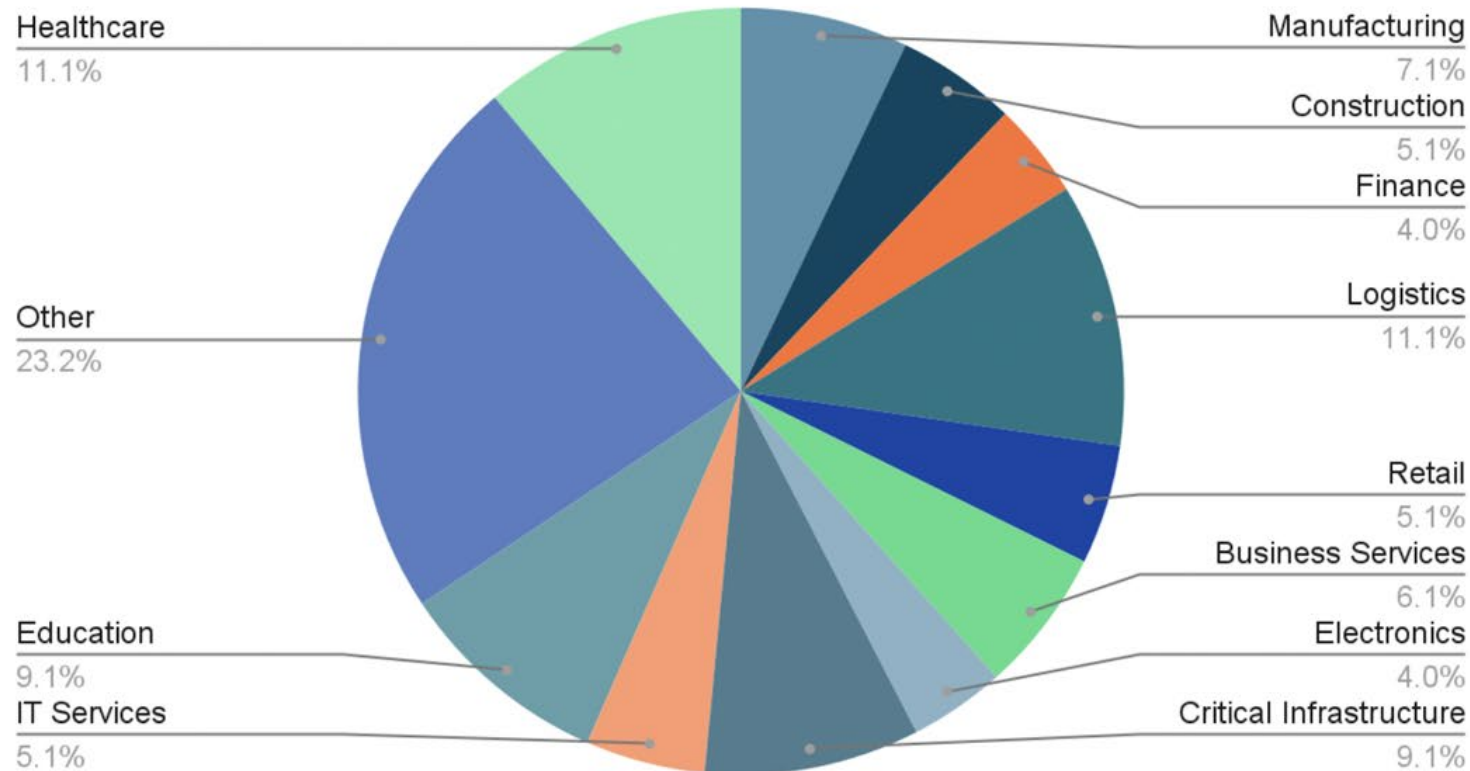
Ransomware Victimology (January 2022)



Recorded Future®

Ransomware

Ransomware Victimology (August 2022)



Recorded Future®

Conclusions





Questions?

 Recorded Future®