

# ADVANCED PENETRATION TESTING NON-WESTERN IT INFRASTRUCTURES



# ROLL CALL

STEVE BOROSH IS A US ARMY INFANTRY VETERAN WHO ALSO OPERATED AS PERSONAL SECURITY IN AFGHANISTAN AND STARTED HACKING THE PLANET WITH BLACK HILLS INFORMATION SECURITY IN 2021. STEVE HAS BEEN INSTRUCTING OFFENSIVE COURSES SINCE 2015. HE HAS INSTRUCTED AT CONFERENCES SUCH AS BLACKHAT AND WILD WEST HACKIN' FEST, FOR FORTUNE 500 COMPANIES, AND FOR FEDERAL LAW ENFORCEMENT. HE ENJOYS RELEASING SHOCK-AND-AWE RESEARCH BLOGS AND OPEN-SOURCE TOOLS TO DRIVE CHANGE IN THE INDUSTRY. YOU MAY FIND STEVE RUNNING THE BEACH, HIKING A MOUNTAIN, OR HANGING OUT WITH HIS HANDSOME UKRAINIAN MAINE COON CATS.



# TALK OVERVIEW

MOST OFFENSIVE-RELATED CYBERSECURITY COURSES AND TALKS TODAY ARE TAILORED TO FOCUS ON WESTERN INFORMATION TECHNOLOGY SYSTEMS. PRIMARILY, ENGLISH-BASED SOFTWARE AND SYSTEMS RUNNING ON-PREMISES OR HOSTED IN CLOUD INFRASTRUCTURE, OWNED BY WESTERN-BASED COMPANIES, RESIDING WITHIN US OR EU BORDERS. THIS COURSE HAS BEEN DESIGNED FOR THOSE CHARGED WITH HELPING TO SECURE NON-WESTERN IT SYSTEMS BY WAY OF PENETRATION TESTING. THIS COURSE AND ASSOCIATED LABS WILL COVER A RANGE OF TECHNOLOGIES, LANGUAGES, SOFTWARE, AND SERVICES THAT A PENETRATION TESTER MAY ENCOUNTER WHILE ENGAGING VARIOUS THEORETICAL NON-WESTERN ORGANIZATIONS AND THE DIFFERENT CHALLENGES EACH MAY BRING. MOST IMPORTANTLY, THIS COURSE WILL PROVIDE YOU WITH THE NECESSARY MINDSET AND FLEXIBLE TTP'S TO EFFICIENTLY AND EFFECTIVELY ASSESS THE SECURITY OF ANY NON-WESTERN IT INFRASTRUCTURE.



# DISCLAIMER

- Unauthorized activities may have legal ramifications, or worse... (might catch a bad case of polonium-210 (Alexander Litvinenko))



# OBJECTIVES

- STUDENTS SHOULD LEARN HOW TO BE ADAPTABLE TO EFFECTIVELY OPERATE AGAINST ORGANIZATIONS WITH NON-WESTERN HARDWARE, NON-ENGLISH SOFTWARE, DATA, OR SYSTEMS INDEPENDENT OF LANGUAGE CONSTRAINTS.
- NO PHISHING OR SOCIAL ENGINEERING.

# WESTERN VS NON-WESTERN NETWORKS

## WESTERN NETWORKS

- ENGLISH WINDOWS.
- ACTIVE DIRECTORY.
- CLOUD AZURE/AWS
- CISCO HARDWARE.
- VARIOUS EDR VENDORS. (CLOUD HEAVY)
- INTEL/AMD ARCH
- MS OFFICE

## NON-WESTERN NETWORKS

- NON-ENGLISH WINDOWS.
- ALDPRO OR LDAP.
- YANDEX (RU), BAIDU (CN)
- HUAWEI
- KASPERSKY (LOCAL UPDATES).
- ELBRUS (DOMESTIC RUSSIAN CPU).
- LOONGSON, ZHAOXIN (DOMESTIC CHINA CPU)
- LIBREOFFICE, MYOFFICE/R7-OFFICE (RUSSIA)
- KINGSOFT WPS OFFICE (JINSHAN WPS OFFICE), AND YOZOSOFT OFFICE. (CHINA GOV).

Government	Key IT System(s)	Description
China	Kylin OS (NeoKylin variant)	A Linux-based domestic OS developed by the National University of Defense Technology, pre-installed on most government computers. In 2024, China banned Windows, Intel, and AMD in official systems to promote local tech like Kylin and HarmonyOS. It supports over 4,000 software/hardware products and emphasizes data sovereignty.
Russia	Astra Linux	A Debian-based Linux distribution certified for government and military use, replacing Windows amid Western sanctions. Deployed across ministries (e.g., Internal Affairs purchased 3,000 units in 2022) and the armed forces for secure operations.
North Korea	Red Star OS	A highly modified Linux distribution developed since 1998 by the Korea Computer Center. It's mandatory for government and state computers, featuring built-in surveillance to detect Western media or tampering, with no internet access for users.

# WHAT IS “NON-WESTERN” IT INFRASTRUCTURE?



**Cuba** Nova Linux

An Ubuntu-based OS launched in 2009 by the University of Informatics Sciences. Used in government offices to counter U.S. tech restrictions; a lightweight version (Nova Lightweight) targets low-end hardware for broader adoption.

**India** BOSS GNU/Linux and Maya OS

BOSS (Bharat Operating System Solutions) is a customized Linux for federal use, supporting Indian languages. Maya OS (Ubuntu-based) is mandated for the Ministry of Defence's internet-connected systems since 2023. Adopted post-Windows XP end-of-life.

**Venezuela** Canaima

A Debian-based Linux distribution rolled out since 2004 via Decree 3390, prioritizing free software in public administration. Distributed to schools and offices for cost savings and independence from proprietary systems.

**Turkey** Pardus Linux

A government-developed Linux distro since 2003 by the National Research Institute of Electronics and Cryptology. Used in public sector desktops and servers, with versions supporting Turkish localization and security features.

# WHAT IS “NON-WESTERN” IT INFRASTRUCTURE?





Country	OS	Download Type	Link	Notes
China	Kylin OS (NeoKylin)	ISO (v6.0 Desktop)	<a href="#">NeoKylin 6</a>	Older version; English partial support. For a modern open-source variant, use openKylin ISO from <a href="#">official site</a> . Integrates with Huawei/ZTE networking via standard Linux drivers.
Russia	Astra Linux	ISO (v2.12 Common Edition)	<a href="#">Official Mirror</a>	Full edition for labs; supports Eltex/NTC Vulkan simulation via virtio networking. Free registration may be required for latest.
North Korea	Red Star OS	ISO (v3.0 English/Korean)	<a href="#">Archive.org Download</a>	Modified for foreigners; includes built-in surveillance—run isolated. Compatible with Glocom-like comms via emulated Ethernet. Modded version on <a href="#">GitHub</a> .
Cuba	Nova Linux	ISO (v9.0 Escritorio AMD64)	<a href="#">Official Mirror</a>	Desktop variant; lightweight for VMs. Other editions: Ligero, Servidor v8. Ties into Huawei/ETCSA via open-source tools.
India	BOSS GNU/Linux	ISO (Latest Desktop/Server)	<a href="#">Official Downloads</a>	Supports x86/AMD64; multilingual for Indian defense sims. BEL/Signaltron networking via kernel modules.
India	Maya OS	N/A (Restricted)	Not publicly available	Defense-only; no ISO for civilians. Use BOSS as proxy for similar stack testing.
Venezuela	Canaima	ISO (v2.1 DVD i386/AMD64)	<a href="#">Official Site</a>	Full DVD image; SourceForge mirror at <a href="#">project page</a> . ZTE/Huawei integration via Debian repos.
Turkey	Pardus Linux	ISO (v23.2 XFCE/GNOME)	<a href="#">Official Download</a>	Multiple DEs; server edition available. Aselsan TASMUS sim via standard virtnet.

# OS DOWNLOADS



# WHAT THIS MEAN FOR PENETRATION TESTERS?

- SENSITIVE NON-WESTERN NETWORKS HAVE BEEN MOVING AWAY FROM WINDOWS ECOSYSTEMS FOR YEARS.
- BASICS ARE STILL NEEDED, USER MANAGEMENT, FILE SHARING, OFFICE PRODUCTIVITY, AND REMOTE ACCESS.

NEOKYLIN



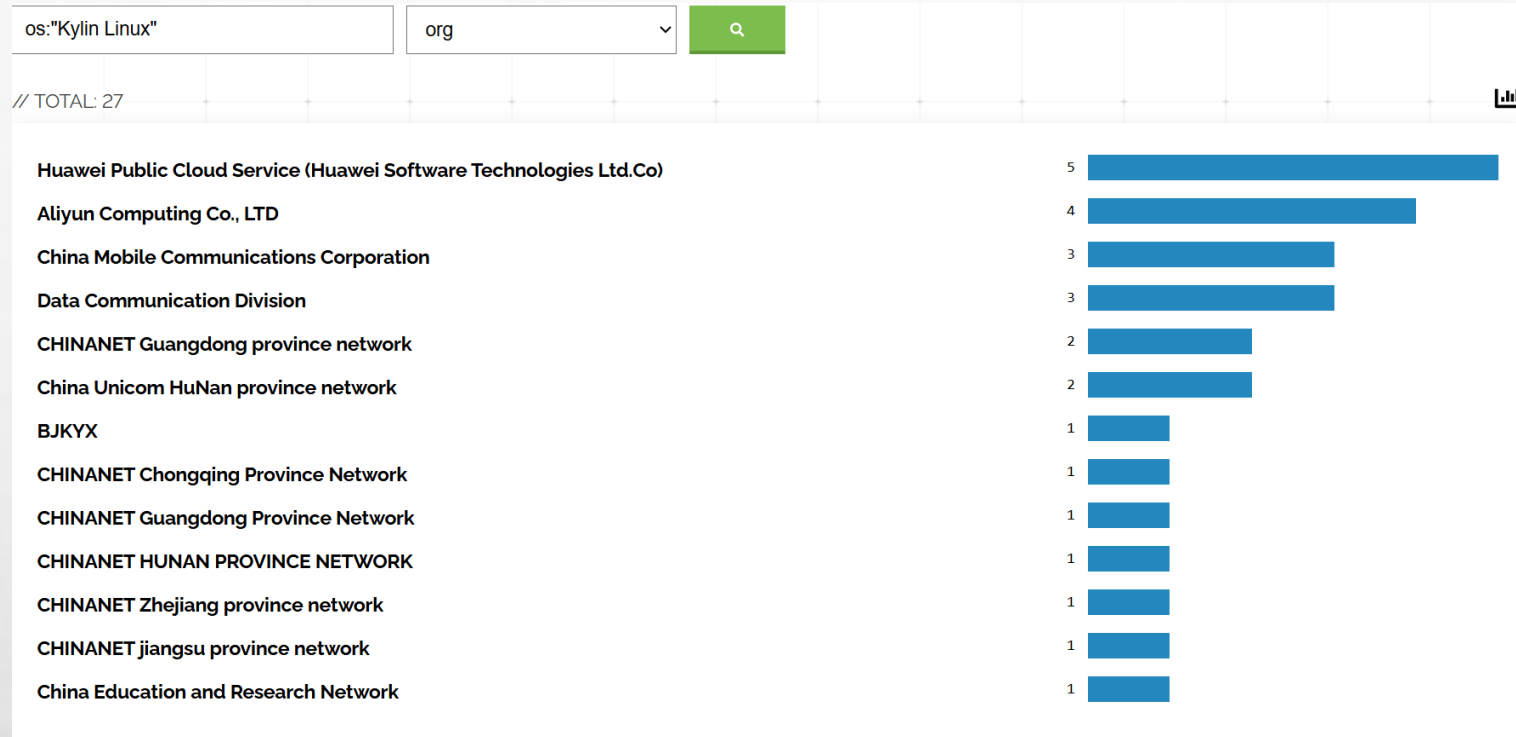
# WHAT IS NEOKYLIN FOR?

- NEOKYLIN IS EXPLICITLY ENGINEERED FOR HIGH-SECURITY ENVIRONMENTS, BUILDING ON THE ORIGINAL KYLIN'S B2 CERTIFICATION WHILE INCORPORATING LINUX-SPECIFIC ENHANCEMENTS FOR MODERN THREATS. IT HAS BEEN DEPLOYED SINCE 2007 ON MILITARY SERVERS TO "HARDEN" NETWORKS AGAINST CYBERWARFARE, MAKING IT IMPENETRABLE TO TOOLS TARGETING COMMON OSes LIKE WINDOWS OR STANDARD LINUX. BY 2019, IT ACHIEVED 90% MARKET SHARE IN CHINA'S GOVERNMENT SECTOR AND COMPATIBILITY WITH OVER 4,000 DOMESTIC HARDWARE/SOFTWARE PRODUCTS, ENSURING SOVEREIGNTY.



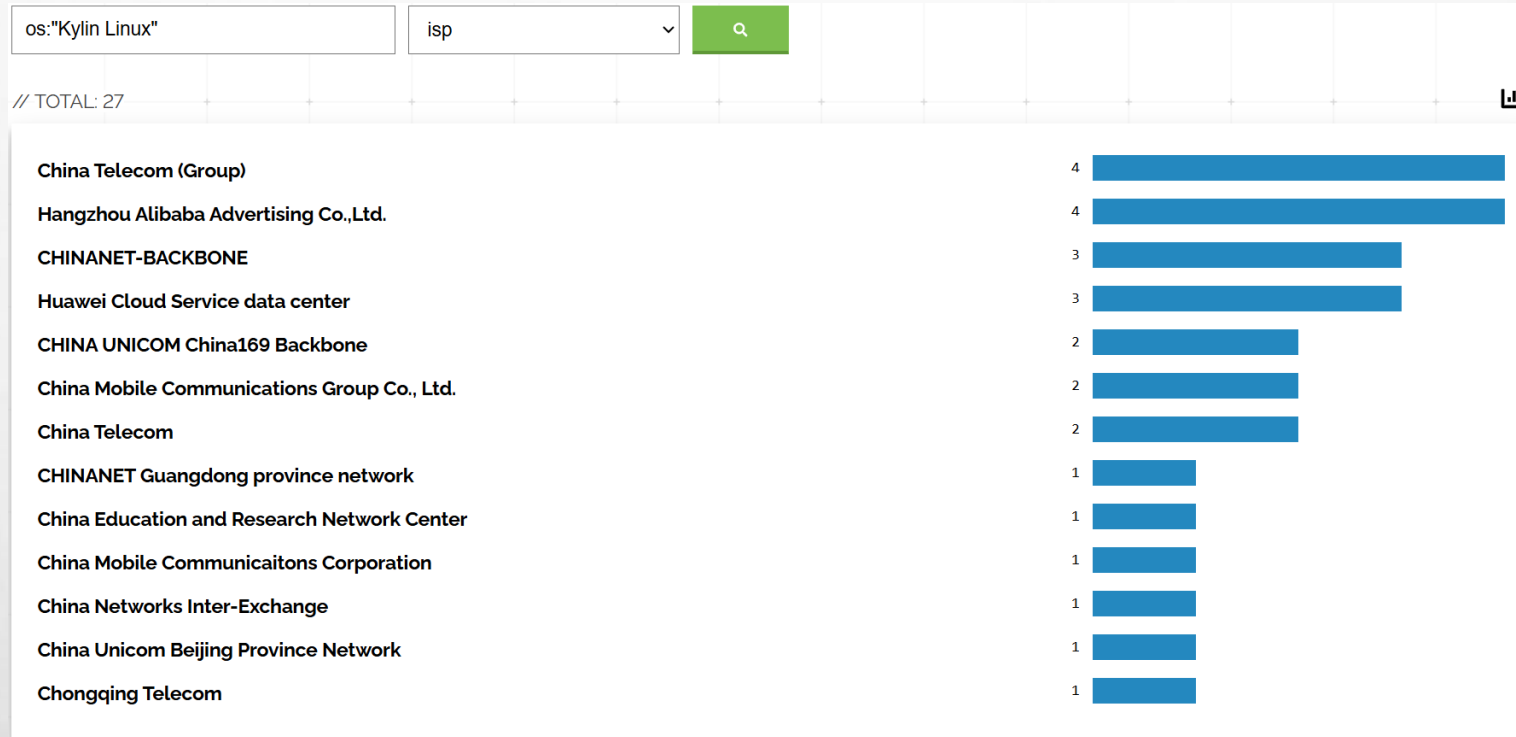
# KEY SECURITY FEATURES OF NEOKYLIN

Feature	Description	Relevance to Government/Military Use
Mandatory Access Control (MAC)	Enforces strict role-based policies to prevent unauthorized data access, similar to SELinux but customized for Chinese standards.	Critical for classified networks; limits lateral movement in breaches, used in PLA command systems.
Multi-Level Security Mechanism	Supports hierarchical security levels (e.g., B2/B3 equivalents), including privilege isolation and fine-grained auditing.	Meets China's national security requirements for military servers; protects against insider threats and espionage.
Unified Security Management Center (SMC)	Centralized tool for encryption, two-factor authentication, network protection, and secure file deletion.	Enables real-time monitoring in defense environments; integrates with domestic CPUs like Feiteng for hardware-level security.
Kernel-Level Hardening	Includes power management for high-performance ops, anti-tampering modules, and compatibility with secure hypervisors.	Powers supercomputers like Tianhe-1/2; optimized for parallel computing in military simulations.
Localization and Compliance	Runs on Chinese processors (e.g., Loongson, Zhaoxin); certified for zero foreign dependencies.	Aligns with PLA mandates to eliminate U.S. tech vulnerabilities; deployed in 70%+ of industrial/military controls.



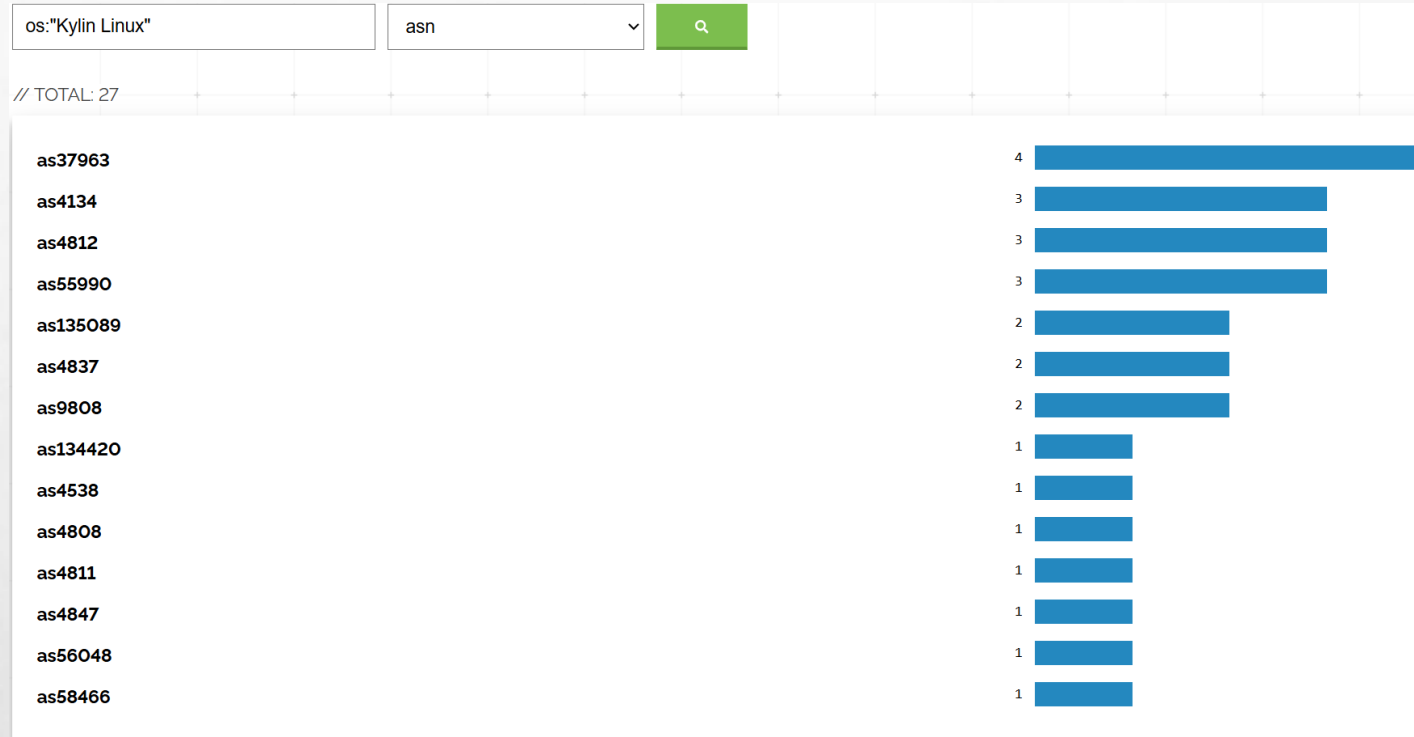
# NEOKYLIN ECOSYSTEM: ORGS





# NEOKYLIN ECOSYSTEM:ISP

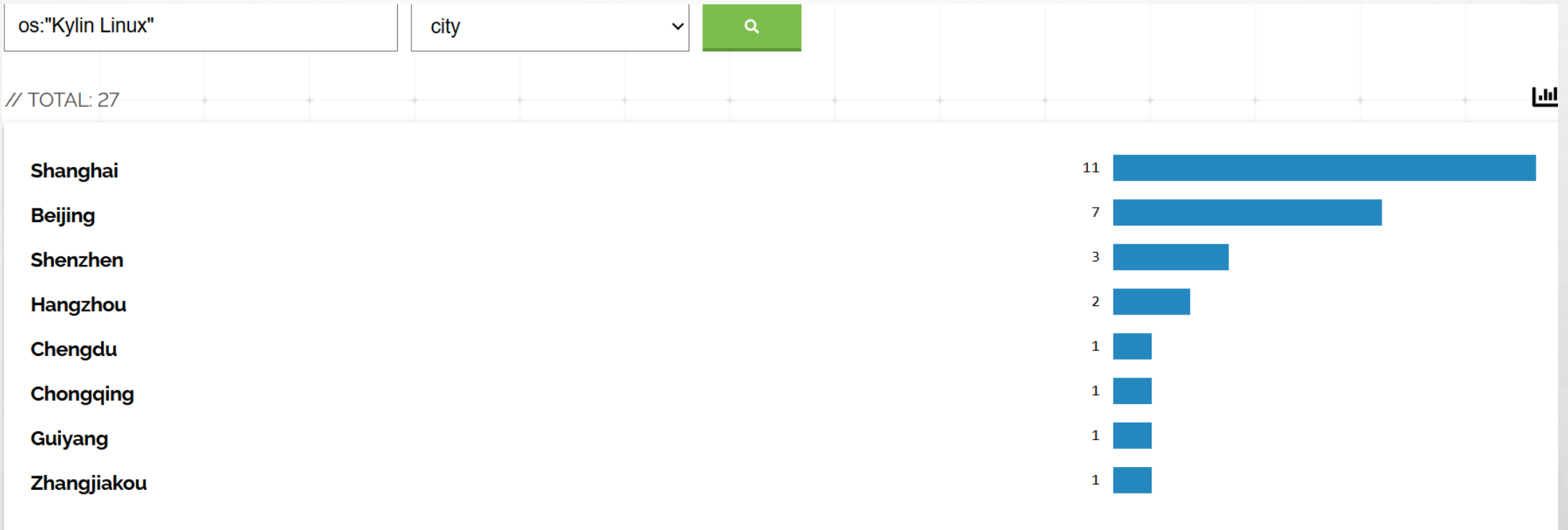




# NEOKYLIN ECOSYSTEM:ASN



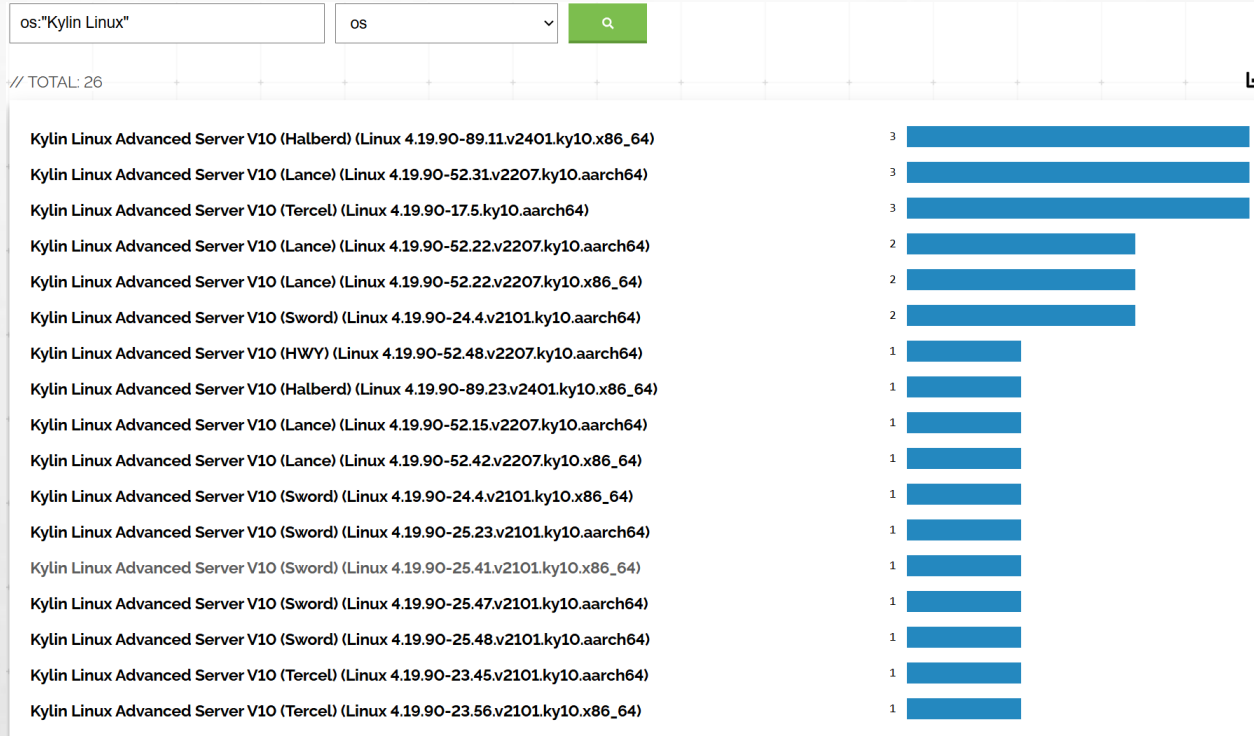




# NEOKYLIN ECOSYSTEM:CITY







# NEOKYLIN ECOSYSTEM:OS VERSION



# ASTRAOS





# KEY SECURITY FEATURES OF ASTRAOS



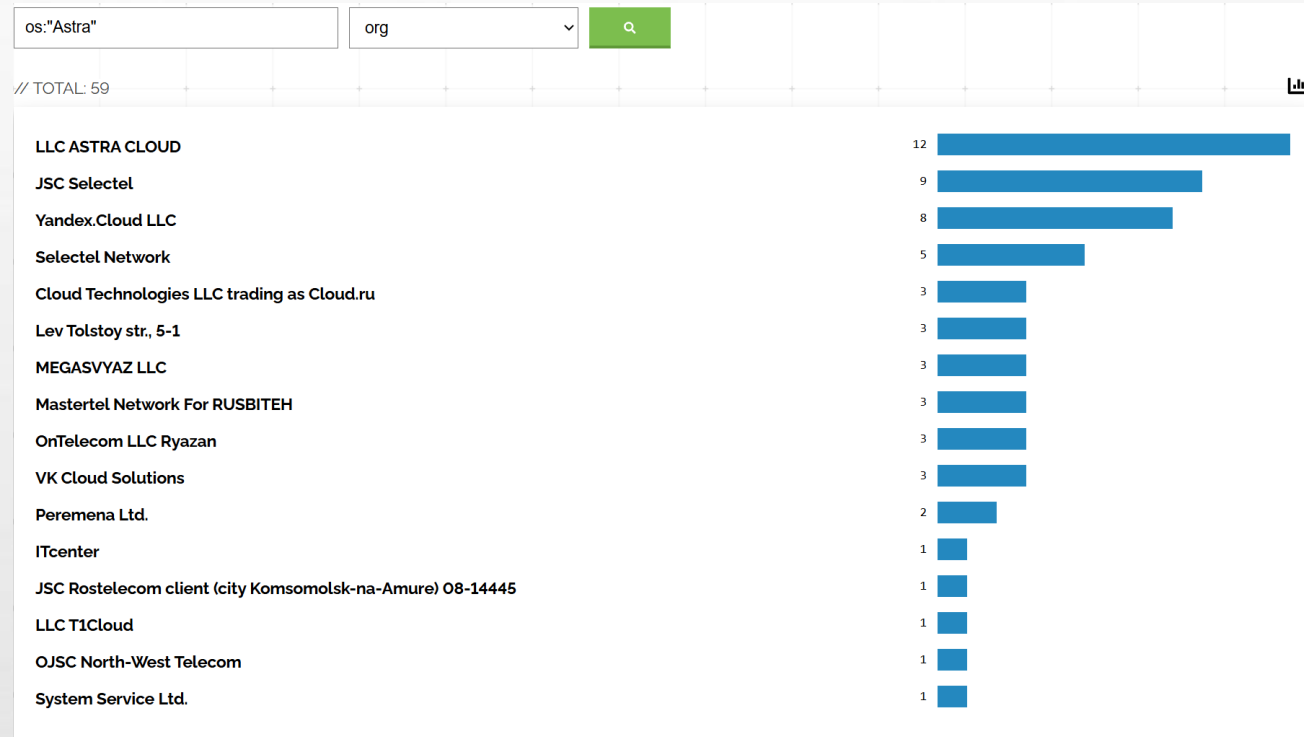
Supports hardened configurations.



Astra's Parsec subsystem (an SELinux variant).

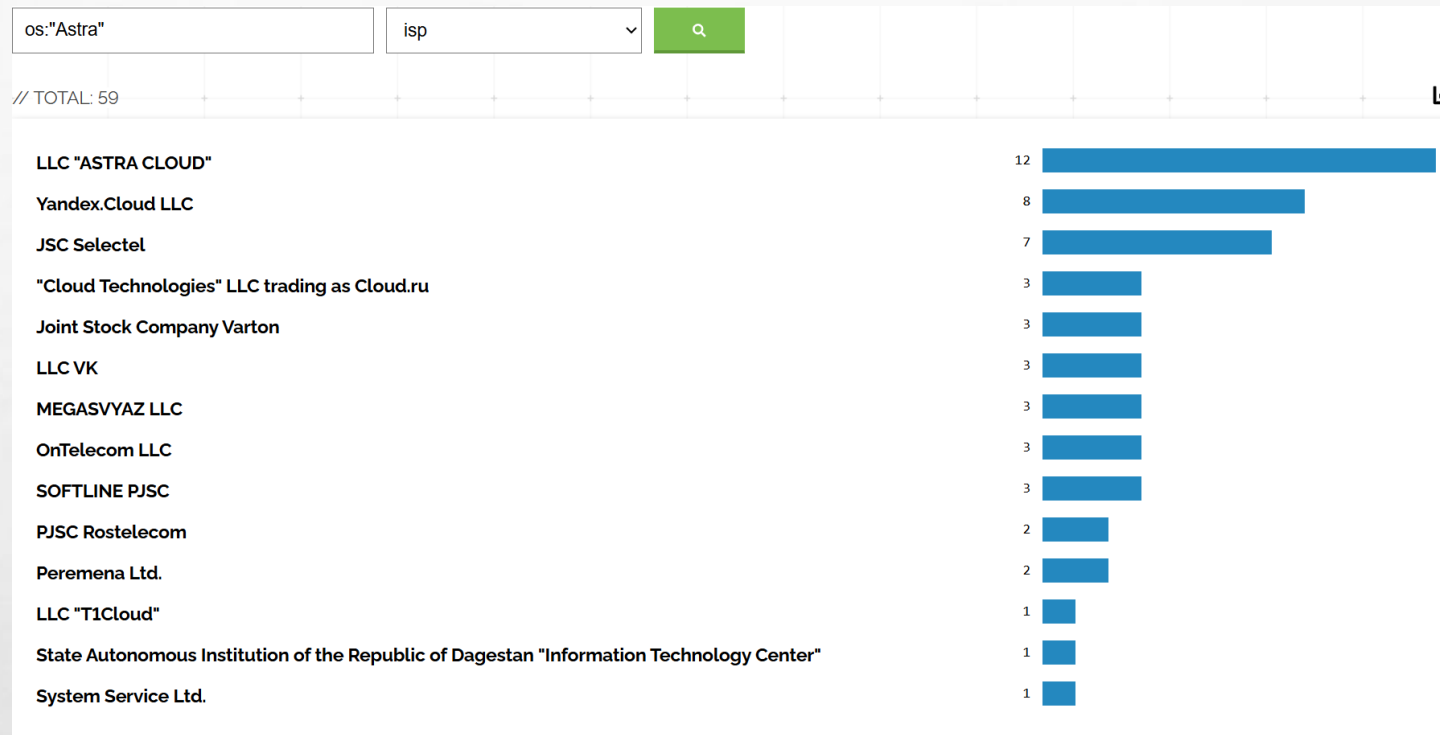


GOST cryptographic standards for data-at-rest, and integration with domestic hardware (e.g., Elbrus processors).



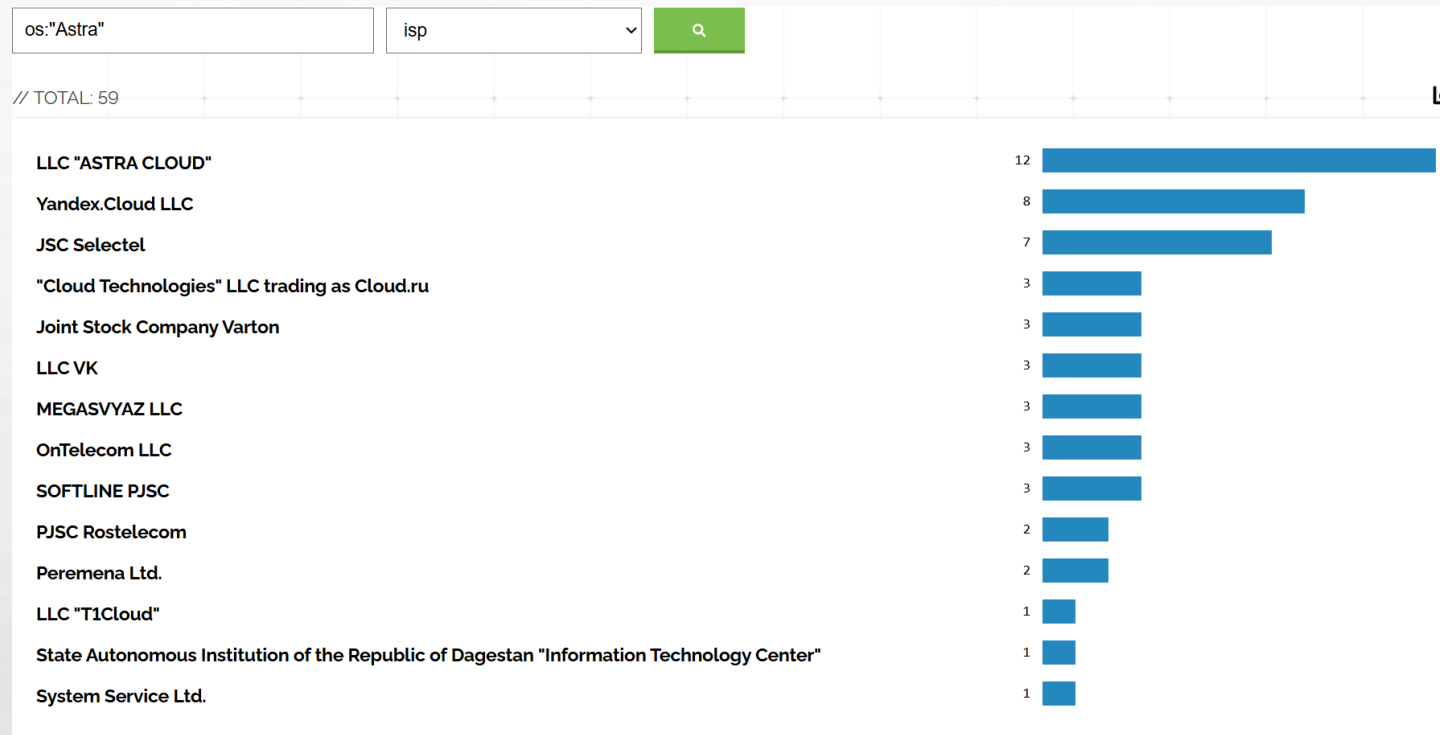
# ASTRA ECOSYSTEM:ORGS





# ASTRA ECOSYSTEM:ISP

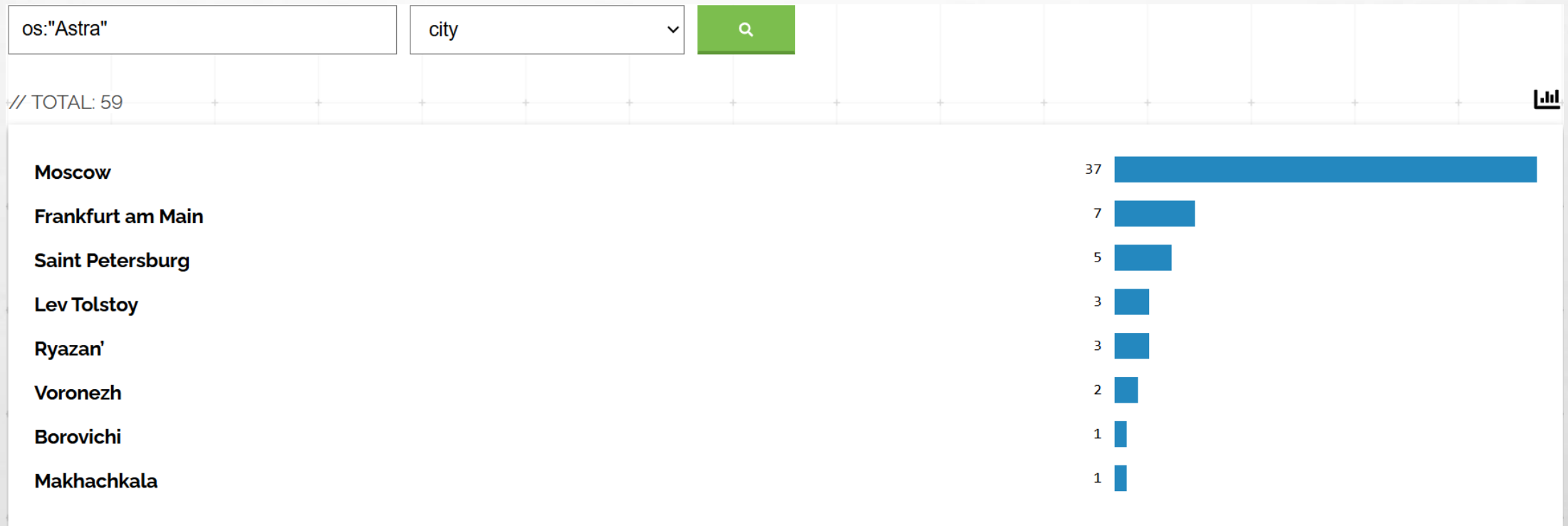




# ASTRA ECOSYSTEM:ASN

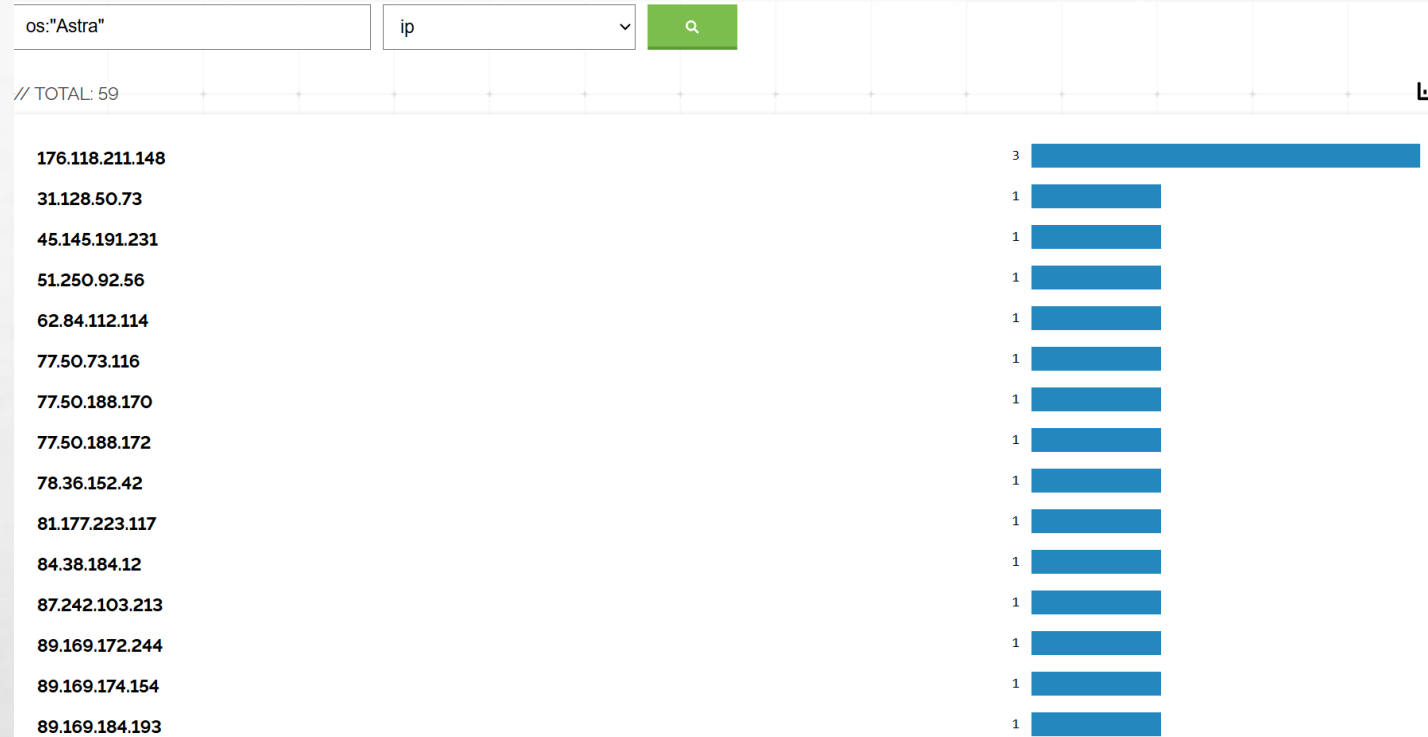






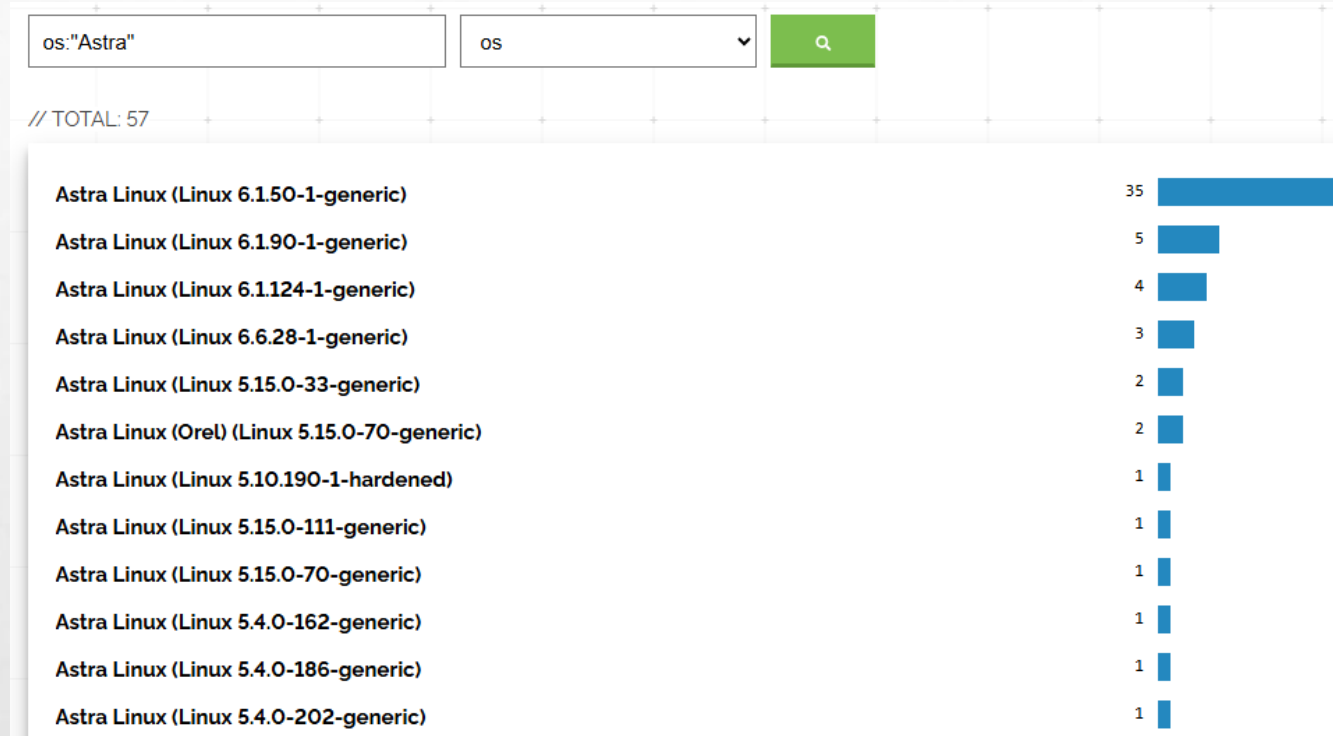
# ASTRA ECOSYSTEM:CITY





# ASTRA ECOSYSTEM:IP





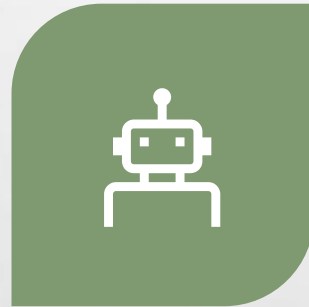
# ASTRA ECOSYSTEM:OS VERSION



# RANGE OVERVIEW AND ACCESS



OSINT LAB



ACTIVE RECON  
LAB



INITIAL ACCESS  
LAB



LATERAL  
MOVEMENT LAB

# OPERATIONAL SETUP



“PROPER PLANNING PREVENTS POOR PERFORMANCE.”



# THE “OODA LOOP” DECISION CYCLE



- CREATED BY RETIRED AIR FORCE COLONEL JOHN BOYD.
- OBSERVE: COLLECT CURRENT INFORMATION FROM MULTIPLE SOURCES TO GAIN SITUATIONAL AWARENESS.
- ORIENT: ANALYZE THE INFORMATION TO MAKE SENSE OF THE SITUATION.
- DECIDE: MAKE A BEST GUESS DECISION AND CONSIDER IT FLUID THROUGHOUT THE PROCESS.
- ACT: IMPLEMENT YOUR DECISION DECISIVELY.
- LOOP AS THE SITUATION DICTATES.

# ACTIVITIES FLOW

- (OBSERVE) OSINT / PASSIVE RECON.
- (OBSERVE) ACTIVE RECON / SCANNING / INTERACTING WITH SITES AND APPLICATIONS.
- (ORIENT) ANALYZE YOUR RESULTS, LIST POTENTIAL VULNERABILITIES OR ATTACK PATHS TO FOLLOW.
- (DECIDE) PICK THE MOST EFFICIENT PATH THAT ACCOMPLISHES THE GOALS OF THE ASSESSMENT WITHIN THE PARAMETERS OF THE RULES OF ENGAGEMENT – “IS EXPLOITATION ALLOWED AND HOW FAR ARE YOU ALLOWED TO GO?”
- (ACT) ENTER THE STEPS OF THE ATTACK, INCLUDING COMMANDS, INTO A TEXT EDITOR, VALIDATE CORRECTNESS, THEN COPY AND PASTE THE CORRECT COMMAND INTO THE TERMINAL.
- REPEAT





# SNIPER/SPOTTER METHOD

- ONE OPERATOR ON KEYS.
- ONE OPERATOR TAKING NOTES, SCREENSHOTS, AND KEEPING COMMS WITH THE TEAM AND LEADERSHIP.
- “SLOW IS SMOOTH, SMOOTH IS FAST.”
- COMMANDS IN TEXT, NOT TERMINAL FIRST.

# ATTACK STATION: OVERVIEW

- OPERATING SYSTEMS
  - OS – MOSTLY MATTERS FOR TOOLING AND/OR OPERATOR COMFORT.
    - UBUNTU IN THIS CLASS.
    - NO NEED TO COMPILE YOUR OWN KERNEL, RAMBO.
    - COULD MATCH THE TARGET NETWORK SYSTEMS. (KYLIN, ASTRAOS, ETC)
  - READY FOR MOST SITUATIONS “MORE TOOLS IN THE TOOLBELT”.
    - LANGUAGE TRANSLATIONS FOR IMAGES, DOCUMENTS, AUDIO, AND TEXT.
  - WHAT CODING LANGUAGES WILL YOU USE?
    - PYTHON (VERSIONS), POWERSHELL, C# BINARIES, ETC.
    - ARE YOU READY TO COMPILE?
  - WINDOWS
    - GREAT FOR PROXYING WINDOWS-ONLY TOOLS.
    - PROXIFIER OR PROXYCAP FOR PROXYING YOUR TOOLS.
    - DNS CAN BE TRICKY.

# ATTACK STATION: OPERATOR PROFILES

- OPERATOR PROFILES
  - OS LANGUAGE SETTINGS.
  - OS KEYBOARD SETTINGS.
  - MULTIPLE USERS.
    - REGIONALIZED.
    - VARIATIONS IN TOOLING FOR DIFFERENT TARGETS.
  - TIME SYNCHRONIZATION WITH TARGET OR MISATTRIBUTED.



# KEYBOARDS

- ACCESS REMOTE TERMINALS (ON-SCREEN KEYBOARD).
- TYPE THE WRONG KEYS IN FOREIGN LAYOUT.



# ATTACK STATION: OPERATOR TOOLS

- HARDWARE
  - GPU(S) CRACKING AND AI LLM.
    - ON-PREM.
    - CLOUD.
- SOFTWARE
  - JOHN THE RIPPER (JTR)
    - JUMBO.
  - HASHCAT
    - MODE-SPECIFIC, NOW WITH AUTO MODE AND FLEXIBLE PYTHON EXTENSIONS.
  - CUSTOM
    - FOR NON-STANDARD HASHES.
- WORDLISTS
  - CUSTOM LANGUAGES.

- CHANGE USER LOCALE AND KEYBOARD SETTINGS
  - BEST TO CREATE MULTIPLE USERS AND PROFILES TAILORED TO THE OPERATION.
  - LIST AVAILABLE LOCALES
    - `LOCALE -A`
  - INSTALL A LOCALE
    - `SUDO APT-GET INSTALL LANGUAGE-PACK-RU`
  - ENABLE A LOCALE FOR CURRENT SESSION (LOGOUT REQUIRED)
    - `SUDO UPDATE-LOCALE LANG=RU_RU.UTF-8`  
`LC_MESSAGES=POSIX`
  - SWITCH BACK TO ENGLISH (LOGOUT REQUIRED)
    - `SUDO UPDATE-LOCALE LANG=EN_US.UTF-8`  
`LC_MESSAGES=POSIX`

# ATTACK STATION: LOCALIZATION SETTINGS

# WORDLISTS

- BASIC LISTS
- THIRD-PARTY LEAKS
- STEALER LOGS
- CUSTOM CREATED
  - ML/AI TUNING
  - [HTTPS://GITHUB.COM/OOAFa/OOAFaSECLISTS](https://github.com/OOAFa/OOAFaSECLISTS)

OOAFA / OOAFASecLists Public

<> Code Issues Pull requests Actions Projects Security Insights

main 1 Branch 0 Tags Go to file <> Code

Joff Thyer RU/ZH dns domains added 60d3abc · last year 23 Commits

Discovery	RU/ZH dns domains added	last year
Passwords	additional RU, and ZH content added	last year
Username	Create ir_shodan_squeegee_usernames.txt	last year
LICENSE	Initial commit	last year
README.md	updated README	last year

# OOAFA SECLISTS





How we translated the wordlists:

1. Using Hugging Face, we located several different models for language translation. Some examples as follows:
    - Helsinki-NLP/opus-mt-en-uk: english to ukrainian
    - Helsinki-NLP/opus-mt-en-zh: english to chinese
    - Helsinki-NLP/opus-mt-en-ar: english to arabic
  2. Each word from fed in batches to the translator pipeline after initializing the pre-trained model.
  3. A translated word was rejected if it was a zero length string, contained a space character, was not translated (English), or was a duplicate of a previously translated word.
- Note: for performance improvements, the translation was executed on a Nvidia/Cuda enabled RTX-3070 GPU card.

# TRANSLATION



# BROWSER EXTENSIONS



## Linguist - web page translator



Web page translation, text translation, dictionary, history, custom translators, all you need to ...



## Location Guard



Hide your geographic location from websites.



## User-Agent Switcher and Manager



Spoof websites trying to gather information about your web navigation to deliver distinct co...

- FIREFOX DOES LOCAL TRANSLATIONS.
- SPOOF JAVASCRIPT GPS.
- BYPASS UA CHECKS TO SERVE SPECIFIC CONTENT (MOBILE UA).
- CAPTCHA BUSTER

# LLM SETUP AND USAGE SCENARIOS

- WHY RUN OUR OWN?
  - SENSITIVE DATA.
  - CUSTOMIZED FLOW.
  - TEXT/IMAGE/DOCUMENT TRANSLATION
  - ATTACK RESEARCH.
- HARDWARE REQUIRED.
- OPENWEBUI.
  - WEB-BASED QUERIES

Main Tasks Libraries Languages Licenses

Other

Tasks



Text Generation



Any-to-Any



Image-Text-to-Text



Image-to-Text



Image-to-Image



Text-to-Image



Text-to-Video



Text-to-Speech

+ 42

Parameters

< 1B 6B 12B 32B 128B > 500B



# HUGGINGFACE

Libraries



PyTorch



TensorFlow



JAX



Transformers



Diffusers



Safetensors



ONNX



GGUF



Transformers.js



MLX



Keras

+ 41

Models 2,116,640

Filter by name



Qwen/Qwen3-Omni-30B-A3B-Instruct



Any-to-Any · 35B · Updated 4 days ago · 43.9k · 462



Qwen/Qwen-Image-Edit-2509



Image-to-Image · Updated 4 days ago · 13.5k · 409



ibm-granite/granite-docling-258M



Image-Text-to-Text · 0.3B · Updated 4 days ago · 60.1k · 724



Wan-AI/Wan2.2-Animate-14B



openbmb/VoxCPM-0.5B



Text-to-Speech · Updated 8 days ago · 4.6k · 697



deepseek-ai/DeepSeek-V3.1-Terminus



Text Generation · 685B · Updated 4 days ago · 4.75k · 264

# OSINT ACTIVITIES OVERVIEW

Overview.

Search Engines.

Scanning by third-party.

DNS discovery.

Certificate transparency.

“Foreign” technology research.

Web of connected entities.



# OVERVIEW

OSINT Methodology is similar except, for requiring localized search results and potential language barriers.

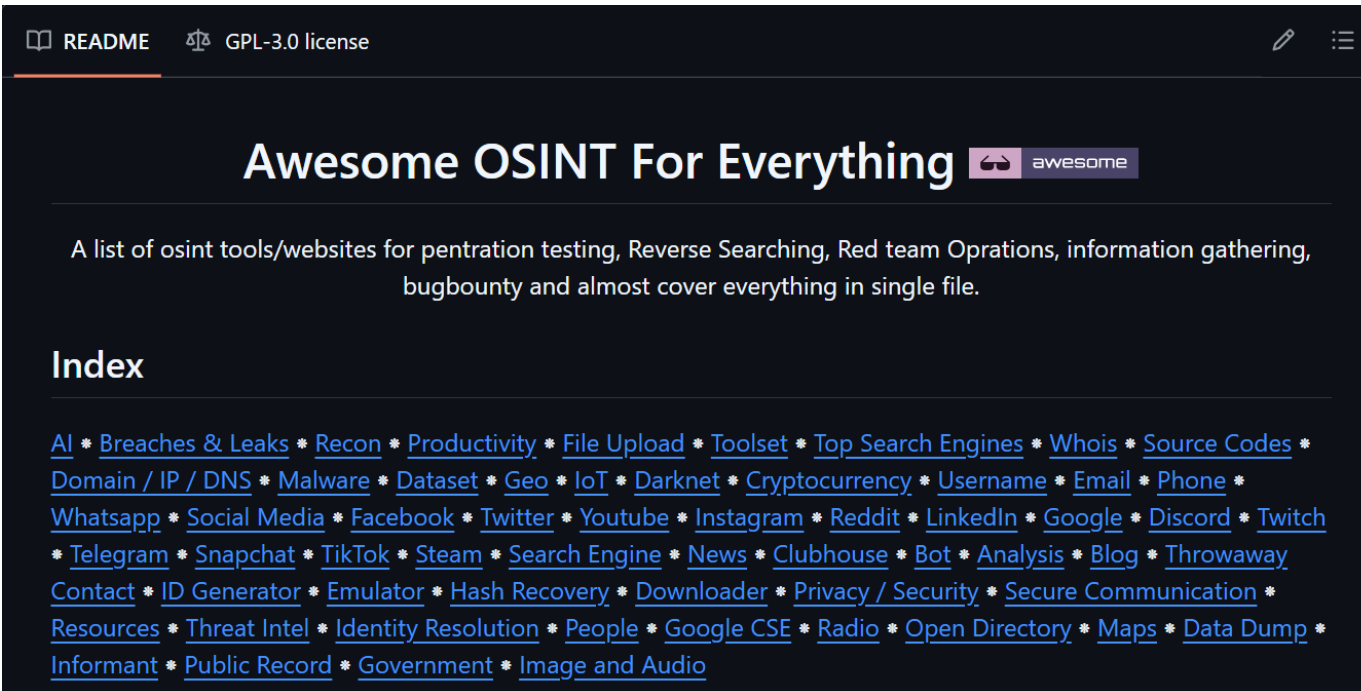
Location-based content served, or on-page translation may serve different content.

User-Agent switching, VPN or Proxy, and browser (JavaScript) location spoofing may be necessary.



# AWESOME OSINT

- GITHUB REPOSITORY
- [HTTPS://GITHUB.COM/ASTROSP/AWESOME-OSINT-FOR-  
EVERYTHING](https://github.com/ASTROSP/awesome-osint-for-everything)



The screenshot shows the README for the 'Awesome OSINT For Everything' repository. At the top, it says 'README' and 'GPL-3.0 license'. The title 'Awesome OSINT For Everything' is prominently displayed with an 'awesome' badge. Below the title, a description states: 'A list of osint tools/websites for penetration testing, Reverse Searching, Red team Operations, information gathering, bugbounty and almost cover everything in single file.' An 'Index' section follows, listing numerous categories and tools as links, including AI, Breaches & Leaks, Recon, Productivity, File Upload, Toolset, Top Search Engines, Whois, Source Codes, Domain / IP / DNS, Malware, Dataset, Geo, IoT, Darknet, Cryptocurrency, Username, Email, Phone, Whatsapp, Social Media, Facebook, Twitter, Youtube, Instagram, Reddit, LinkedIn, Google, Discord, Twitch, Telegram, Snapchat, TikTok, Steam, Search Engine, News, Clubhouse, Bot, Analysis, Blog, Throwaway, Contact, ID Generator, Emulator, Hash Recovery, Downloader, Privacy / Security, Secure Communication, Resources, Threat Intel, Identity Resolution, People, Google CSE, Radio, Open Directory, Maps, Data Dump, Informant, Public Record, Government, and Image and Audio.

README GPL-3.0 license

## Awesome OSINT For Everything

A list of osint tools/websites for penetration testing, Reverse Searching, Red team Operations, information gathering, bugbounty and almost cover everything in single file.

### Index

[AI](#) \* [Breaches & Leaks](#) \* [Recon](#) \* [Productivity](#) \* [File Upload](#) \* [Toolset](#) \* [Top Search Engines](#) \* [Whois](#) \* [Source Codes](#) \* [Domain / IP / DNS](#) \* [Malware](#) \* [Dataset](#) \* [Geo](#) \* [IoT](#) \* [Darknet](#) \* [Cryptocurrency](#) \* [Username](#) \* [Email](#) \* [Phone](#) \* [Whatsapp](#) \* [Social Media](#) \* [Facebook](#) \* [Twitter](#) \* [Youtube](#) \* [Instagram](#) \* [Reddit](#) \* [LinkedIn](#) \* [Google](#) \* [Discord](#) \* [Twitch](#) \* [Telegram](#) \* [Snapchat](#) \* [TikTok](#) \* [Steam](#) \* [Search Engine](#) \* [News](#) \* [Clubhouse](#) \* [Bot](#) \* [Analysis](#) \* [Blog](#) \* [Throwaway](#) \* [Contact](#) \* [ID Generator](#) \* [Emulator](#) \* [Hash Recovery](#) \* [Downloader](#) \* [Privacy / Security](#) \* [Secure Communication](#) \* [Resources](#) \* [Threat Intel](#) \* [Identity Resolution](#) \* [People](#) \* [Google CSE](#) \* [Radio](#) \* [Open Directory](#) \* [Maps](#) \* [Data Dump](#) \* [Informant](#) \* [Public Record](#) \* [Government](#) \* [Image and Audio](#)

# SEARCH ENGINES

Easy starting point

Google Dorks

Yandex

Searching in Russian – Cyrillic and Latin

Specialized Search Engines

VPN/Residential Proxy for local area results.

# ASN/IP DISCOVERY



**RIPE vs ARIN**

<https://www.ripe.net/membership/member-support/the-ripe-ncc-and-ukraine-russia/>



**WHOIS**

<https://www.nic.ru/en/whois/?searchWord=terratech.ru>

# NIC.RU

← → ↻ 📄 nic.ru/en/whois/?searchWord=terratech.ru

 Domains Hosting and servers SSL certificates Sites Safety For large businesses

---

## terratech.ru is taken

**Information according to whois.registry.tcinet.ru**

% TCI Whois Service

domain:	TERRATECH.RU
nserver:	ns1.timeweb.ru.
nserver:	ns2.timeweb.ru.
nserver:	ns3.timeweb.org.
nserver:	ns4.timeweb.org.
state:	REGISTERED, DELEGATED, UNVERIFIED
org:	AO TERRA TEX
taxpayer-id:	7722429553
registrar:	TIMEWEB-RU
admin-contact:	<a href="http://timeweb.name/contact-admin">http://timeweb.name/contact-admin</a>
created:	2010-02-15T21:00:00Z
paid-till:	2025-02-15T21:00:00Z
free-date:	2025-03-19
source:	TCI

Last updated on 2024-04-03T16:46:31Z

# ASN/IP DISCOVERY

- RDAP
  - [HTTPS://ABOUT.RDAP.ORG](https://about.rdap.org)
  - [HTTPS://IPINFO.IO/COUNTRIES/RU#SECTION-ASNS](https://ipinfo.io/countries/ru#section-asns)
- IP BLOCK OWNERSHIP BY CORPORATIONS APPEARS TO BE SOMEWHAT UNCOMMON.

DNS

DNS Map

Whois

Certs

Subdomains

ctrl+1-5

ⓘ

How it works

This is a deduplicated list of all subdomains found in the certificate transparency logs for this domain.

Export

Domain Name	First seen ↑	Still exists
landing.ttk.ru	3/7/2025, 6:37:28 AM	✓
www.landing.ttk.ru	3/7/2025, 6:37:28 AM	✓
b2b.videoportal.ttk.ru	2/26/2025, 5:42:36 AM	✓
ip62-33-2-10.srn.host.ttk.ru	1/8/2025, 6:37:17 PM	✓
career.ttk.ru	10/15/2024, 7:58:34 AM	✓
www.career.ttk.ru	10/15/2024, 7:58:34 AM	✓
digitaldev.ttk.ru	9/25/2024, 3:33:16 AM	✗
ds.ttk.ru	6/5/2024, 2:30:48 AM	✓

DNS Discovery - <https://digger.tools/>





# DNS DISCOVERY CONT.

AMASS

- [HTTPS://GITHUB.COM/OWASP-AMASS/AMASS](https://github.com/OWASP-AMASS/AMASS)

AMASS ENUM -D EXAMPLE.RU -V

AMASS ENUM -D EXAMPLE.RU -ACTIVE -TRF RESOLVERS.TXT -V

AMASS ENUM -D EXAMPLE.RU -ACTIVE -TRF RESOLVERS.TXT /

-BRUTE -W WORDLIST.TXT -V

[HTTPS://GITHUB.COM/OOAFa/OOAFaSECLISTS/](https://github.com/OOAFa/OOAFaSECLISTS/)

[HTTPS://GITHUB.COM/TRICKEST/RESOLVERS](https://github.com/Trickest/resolvers)

# AMASS RESULTS

```
charts.terratech.ru (FQDN) --> a_record --> 83.222.11.192 (IPAddress)
www.pixel-ai.terratech.ru (FQDN) --> a_record --> 83.222.11.194 (IPAddress)
en.terratech.ru (FQDN) --> a_record --> 83.222.11.194 (IPAddress)
billing.terratech.ru (FQDN) --> a_record --> 185.175.46.161 (IPAddress)
terratech.ru (FQDN) --> a_record --> 83.222.11.192 (IPAddress)
www.geovision.terratech.ru (FQDN) --> a_record --> 83.222.11.194 (IPAddress)
radar.terratech.ru (FQDN) --> a_record --> 83.222.11.194 (IPAddress)
www.charts.terratech.ru (FQDN) --> a_record --> 83.222.11.192 (IPAddress)
billing-dev.terratech.ru (FQDN) --> a_record --> 185.175.46.3 (IPAddress)
th-dev.terratech.ru (FQDN) --> a_record --> 185.175.46.3 (IPAddress)
info-flyber.terratech.ru (FQDN) --> cname_record --> lb.bitrix24.site (FQDN)
demo.terratech.ru (FQDN) --> a_record --> 185.156.2.217 (IPAddress)
registry.terratech.ru (FQDN) --> a_record --> 185.175.46.161 (IPAddress)
cloud-dev.terratech.ru (FQDN) --> a_record --> 185.175.46.3 (IPAddress)
geovision.terratech.ru (FQDN) --> a_record --> 83.222.11.194 (IPAddress)
tms.terratech.ru (FQDN) --> a_record --> 185.175.46.161 (IPAddress)
www.en.terratech.ru (FQDN) --> a_record --> 83.222.11.194 (IPAddress)
cloud-old.terratech.ru (FQDN) --> a_record --> 185.156.2.215 (IPAddress)
geotron.terratech.ru (FQDN) --> a_record --> 185.156.0.69 (IPAddress)
dzzen.terratech.ru (FQDN) --> a_record --> 83.222.11.192 (IPAddress)
```

# SCANNING BY PROXY

Shodan.io

Zoomeye.ai

en.fofa.info

Censys.io

*Why different results?*

- *Chinese Firewall*



289,179

TOP CITIES

Moscow	114,406
Saint Petersburg	56,584
Novosibirsk	7,912
Yekaterinburg	6,131
Krasnodar	5,622

[More...](#)


[View Report](#)

[Download Report](#)


[Historical Items](#)

[Browse Images](#)

**Product Spotlight:** We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

**79.143.70.197** 

[OKBPROGRESS](#)

 Russian Federation, Moscow

   IIS

**eo1-os**

HTTP/1.1 401 Unauthorized

Content-Type: text/plain; charset=utf-8

Server: Microsoft-IIS/8.0

SPRequestGuid: b4bfc9a1-0ed5-30d4-9312-028ab93f9046

request-id: b4bfc9a1-0ed5-30d4-9312-028ab93f9046

X-FRAME-OPTIONS: SAMEORIGIN

SPRequestDuration: 4

SPIisLatency: 0

WWW-Authenticate: NTLM

WWW-Aut...

# SHODAN.IO QUERY



os = "windows" ✕ && country = "ru" ✕ Not satisfied with the search, try [ZoomEyeGPT](#)

About 6,291,638 results (Nearly year: 505,353 results) 0.148 seconds

Result

Report

Maps

Only \$500

Download All

Subscribe

Tokenizer

Collection

188.35.5.72:9083

9083

msdtc

188.35.5.72

Russia, Moscow Oblast, Dolg...

OS: Windows

Hostname: host-188-35-5-72.net...

Organization: Corporate Internet ...

ASN: AS59793

2025-09-27 14:13

Please login to view detail!

Login



#### SEARCH TYPE

Devices 6,272,370 ▼

Ipv4 6,272,295

Ipv6 75

# ZOOMEYE QUERY



country="RU" && os="windows"



AI Lab

Pricing

Support



Favicon(10):

 999+

 999+

 999+

 999+

 999+

 999+

 999+

 701

 530

 520

 505

More

Select all



all

451,210 results ( 138,046 unique IP ) ,589 ms ,Keyword Search.

Nearly year results, click to view [all](#) results.

Intelligently excluded [84](#) Honeypot/Fraud Datas, [click](#) to view



API



TOP FID



tc088... 107,680

uk9... 33,307

... 12,18

Z400... 21,359

B2GS... 15,756

TOP COUNTRIES/REGIONS

>> RU  451,210



<https://vshb.club>

185.41.187.141

 Russian Federation  
ASN: 48347

Organization: JSC Mediasoft ekspert

vshb.club

2025-09-27

Apache/2.4.59 (Win32) PHP/7.2.9 OpenS

/ windows

Header

Products

HTTP/1.1 200 OK

Connection: close

Transfer-Encoding: chunked

Cache-Control: post-check=0, pre-check=0

Content-Type: text/html; charset=windows-1251

Date: Sat, 27 Sep 2025 06:11:44 GMT

Expires: Thu, 21 Jul 1977 07:30:00 GMT

Last-Modified: Sat, 27 Sep 2025 06:11:44 GMT

# SCANNING BY PROXY: FOFA

<https://github.com/fofa-info/awesome-fofa>



Server Model: HPE ProLiant DL360 Gen10  
FSMO: PDC  
AD Site: Melkisarovo-2016

RemoteM

Active Directory Users and Computers

File Action View Help

Active Directory Users and Com

msk.aeroflot.ru

Builtin

CardReaders

Computers

Contractors

CUP

Default

Domain Admins

Domain Controllers

Domain Groups

Domain Servers

Domain ServiceAccounts

Domain Users

AdminsAccounts

ExchangeAccounts

ExchangeRooms

ServiceAccounts

Temporary

VPN

Domain Workstations

ForeignSecurityPrincipal

IntelAMT

LK

Managed Service Account

Representation

RMAD-test\_MSK\_OU

ROOT

SVO1

Terminated

Test

Test pwdchange

Users

Name	Type	Description	Office Communications Server Address
afl.api-pnr	User	ВНИМАНИЕ! Использо...	sip:afl.api-pnr@aeroflot.ru
afl.oren	User	ВНИМАНИЕ! Использо...	
afl_ias_ka	User	ВНИМАНИЕ! Использо...	
afl_repair	User	ВНИМАНИЕ! Использо...	
afl_rpa	User	ВНИМАНИЕ! Использо...	
afl_rpa_od	User	ВНИМАНИЕ! Использо...	
afl_zit	User	ВНИМАНИЕ! Использо...	sip:afl_zit@aeroflot.ru
aflamoreq	User	ВНИМАНИЕ! Использо...	sip:aflamoreq@aeroflot.ru
aflbonussupport	User	ВНИМАНИЕ! Использо...	
aflcase	User	ВНИМАНИЕ! Использо...	sip:aflcase@aeroflot.ru
aflcrm-monitoring	User	ВНИМАНИЕ! Использо...	
aflcrm-pkl-dev	User	ВНИМАНИЕ! Использо...	
aflcrm-pkl-preprod	User	ВНИМАНИЕ! Использо...	
aflcrm-pkl-test	User	ВНИМАНИЕ! Использо...	
aflcrm-sds-dev	User	ВНИМАНИЕ! Использо...	
aflcrm-sds-preprod	User	ВНИМАНИЕ! Использо...	
aflcrm-sds-test	User	ВНИМАНИЕ! Использо...	
aflifpl	User	ВНИМАНИЕ! Использо...	
aflimeteo	User	ВНИМАНИЕ! Использо...	sip:aflimeteo@aeroflot.ru
aflinav	User	ВНИМАНИЕ! Использо...	sip:aflinav@aeroflot.ru
afllops	User	ВНИМАНИЕ! Использо...	
aflprivacyoffice	User	ВНИМАНИЕ! Использо...	sip:aflprivacyoffice@aeroflot.ru
aflsales	User	ВНИМАНИЕ! Использо...	sip:aflsales@aeroflot.ru
aflsvo1	User	ВНИМАНИЕ! Использо...	sip:aflsvo1@aeroflot.ru
aflsvo10	User	ВНИМАНИЕ! Использо...	sip:aflsvo10@aeroflot.ru
aflsvo11	User	ВНИМАНИЕ! Использо...	sip:aflsvo11@aeroflot.ru
aflsvo12	User	ВНИМАНИЕ! Использо...	sip:aflsvo12@aeroflot.ru
aflsvo13	User	ВНИМАНИЕ! Использо...	sip:aflsvo13@aeroflot.ru
aflsvo14	User	ВНИМАНИЕ! Использо...	sip:aflsvo14@aeroflot.ru
aflsvo15	User	ВНИМАНИЕ! Использо...	sip:aflsvo15@aeroflot.ru
aflsvo16	User	ВНИМАНИЕ! Использо...	sip:aflsvo16@aeroflot.ru
aflsvo2	User	ВНИМАНИЕ! Использо...	sip:aflsvo2@aeroflot.ru
aflsvo3	User	ВНИМАНИЕ! Использо...	sip:aflsvo3@aeroflot.ru


Activate Windows

Go to Settings to activate Windows.

ENG

28.07.2025

AEROFLLOT HACK



# SCANNING BY PROXY TIPS

- SEARCH WITH BOTH CYRILLIC AND LATIN CHARACTERS.
- SEARCH FOR THIRD-PARTY REFERENCES.
- SEARCH FOR N-DAYS/VULNS.
- PULL INTERNAL DOMAIN NAME AND HOST NAMING SCHEMES FROM NTLM ENDPOINTS

# CERTIFICATE TRANSPARENCY



Censys, cert.sh, etc



<https://github.com/UnaPibaGeek/ctfr>



```
python3 ctfr.py -d terratech.ru
```

```
[!] ---- TARGET: terratech.ru ---- [!]  
  
[-] *.terratech.ru  
[-] *.terratech.ru  
terratech.ru  
[-] billing-dev.terratech.ru  
cloud-dev.terratech.ru  
th-dev.terratech.ru  
[-] billing.terratech.ru  
cloud.terratech.ru  
[-] charts.terratech.ru  
[-] desert.terratech.ru  
[-] dokagi.terratech.ru  
www.dokagi.terratech.ru  
[-] dzzen.terratech.ru  
www.dzzen.terratech.ru  
[-] en.terratech.ru  
www.en.terratech.ru  
[-] flyber.terratech.ru  
[-] geoanalytics.terratech.ru  
geonovosti.terratech.ru  
www.geonovosti.terratech.ru  
[-] geonovosti.terratech.ru  
www.geonovosti.terratech.ru
```



# CERTIFICATE TRANSPARENCY

SUBDOMAINS INDICATE:

TECHNOLOGIES

INTERNAL HOSTNAMES

DEVELOPMENT HOSTS



© 2008 – 2024 PJSC Astra Group

## SOCIAL MEDIA

- REGIONAL RESTRICTIONS / DIFFERENT CONTENT SERVED
  - LINKEDIN, FACEBOOK/INSTAGRAM, TWITTER, TIKTOK
- TELEGRAM
- FORUMS
- RUSSIAN PLATFORMS
  - VKONTAKTE (VK)
  - ODNOKLASSNIKI (OK)
- OTHER NON-WESTERN PLATFORMS
- DISINFORMATION AND REPUTATION DAMAGE



# FOREIGN TECHNOLOGY RESEARCH

## Third-Party Scanning .ru OS Analysis

- Shodan & ZoomEye

## Understanding OS install types

- [Server 2016 ISO Languages](#)
- [How to add language packs](#)

## Edge Devices

- Case: [Phineas Phisher](#)

# WEBSITE RECON

- MAIN WEBSITE
  - [HTTP://WWW.ALMAZ-ANTEY.RU/](http://www.almaz-antey.ru/), YES HTTP
  - NOTICE DIFFERENCE WHEN SWITCHING LANGUAGES USING THE WEBSITE'S FEATURES VS USING THE BROWSER TO TRANSLATE

# WEBSITE RECON – TRANSLATION



Differences when switching languages using the website's features vs using the browser or an extension to translate



Extensions

OpSec  
Accuracy/Clarity



Feature of Website

Accuracy  
Content

# ENGLISH VERSION

MAIN PRODUCT  
RANGE

SCIENTIFIC AND TECHNICAL  
ACTIVITY

PRODUCTION  
ACTIVITIES

MILITARY-TECHNICAL  
COOPERATION

DIVERSIFICATION

STAFF AND SOCIAL  
POLICY

RUS  
ENG

## Russian Version\*

MAIN  
PRODUCTS

SCIENTIFIC AND  
TECHNICAL  
ACTIVITIES

PRODUCTION  
ACTIVITIES

MILITARY-  
TECHNICAL  
COOPERATION

DIVERSIFICATION

PERSONNEL  
AND SOCIAL  
POLICY

INFORMATION  
FOR THE MEDIA

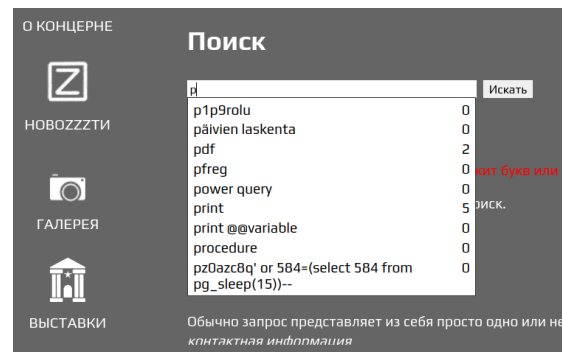
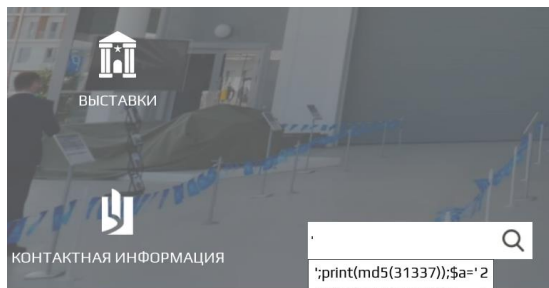
ANTI-  
CORRUPTION

RUSSIAN  
ENG

\*translated by browser

# HTTP AND AUTO-FILL

- %27
- PEOPLE
- PASSES
- ETC





site:almaz-antey.ru



almaz-antey.ru

<http://journal.almaz-antey.ru> > view · [Translate this page](#) ⋮

### Оценка энергетического выигрыша при обнаружении ...

by СМ Костромицкий · 2022 · Cited by 4 — Основой предлагаемого метода является значительное снижение порога обнаружения (условно, в k раз) при малой энергетике...



almaz-antey.ru

<http://journal.almaz-antey.ru> > view · [Translate this page](#) ⋮

### Электролитно-плазменное полирование ...

by СВ Захаров · 2017 · Cited by 8 — В первом случае катодом является ванна 2, во втором - сопло 5 или специальный электрод, находящийся в электрическом контакте со струей...



almaz-antey.ru

<http://journal.almaz-antey.ru> > view · [Translate this page](#) ⋮

### Метод опорных векторов в задаче тепловой ...

by СУ Увайсов · 2022 — Метод опорных векторов относится к группе граничных методов, которая определяет классы при помощи границ областей. В теории искусственных...

# WEBSITE RECON: SITE DORK

SITE:ALMAZ-ANTEY.RU

Quick Search

Show 15 ▼

Date Added Dork

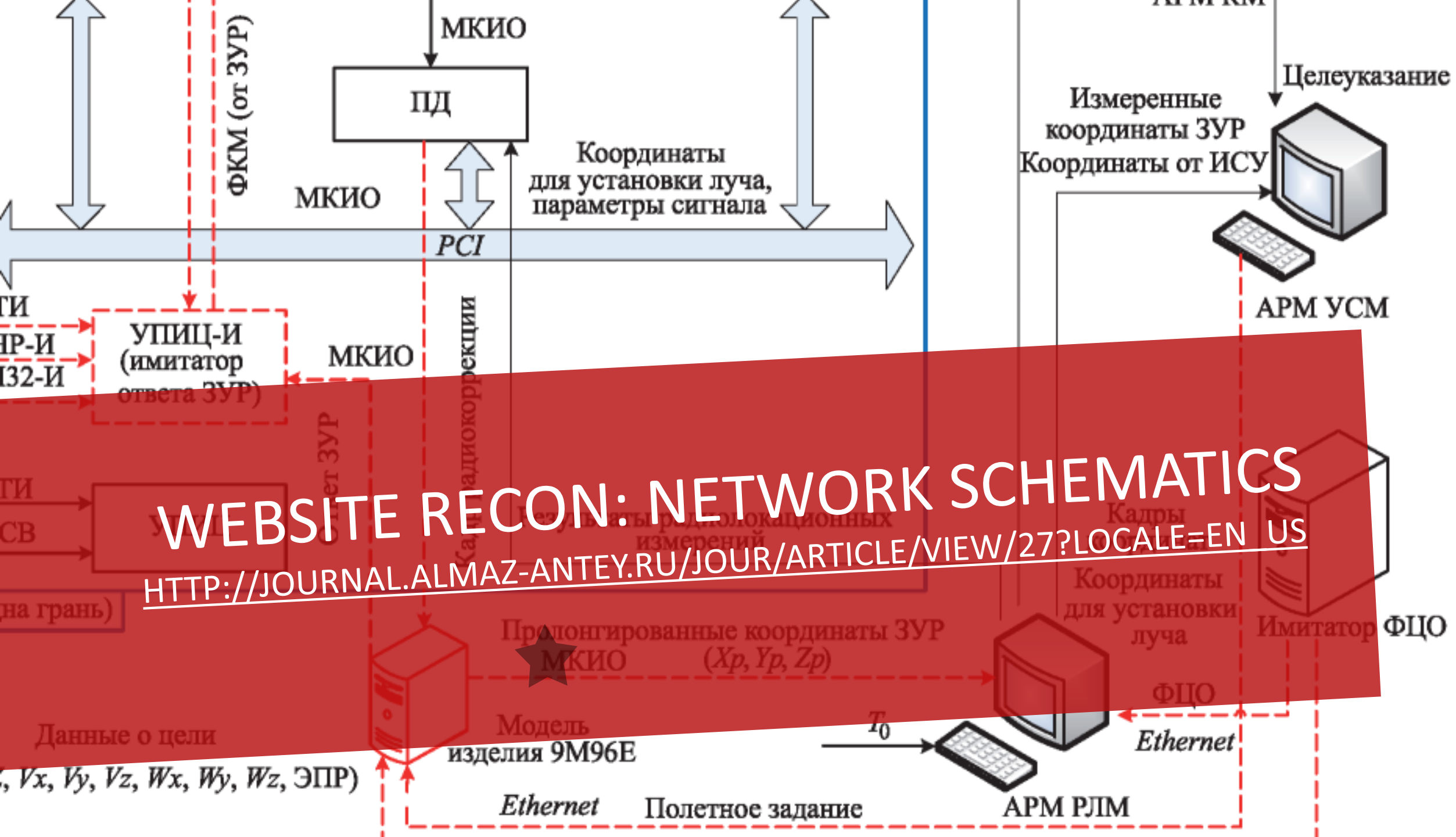
Category

2024-08-23	site:github.com "BEGIN OPENSSH PRIVATE KEY"	Files Containing Passwords
2024-08-23	ext:nix "BEGIN OPENSSH PRIVATE KEY"	Files Containing Passwords
2024-07-26	inurl:home.htm intitle:1766	Various Online Devices
2024-07-04	intitle:"SSL Network Extender Login" -checkpoint.com	Vulnerable Servers
2024-07-04	intext:"siemens" & inurl:"/portal/portal.mwsl"	Vulnerable Servers

# GHDB

[HTTPS://WWW.EXPLOIT-DB.COM/GOOGLE-HACKING-DATABASE](https://www.exploit-db.com/google-hacking-database)





# ROBOTS

- ADMIN PAGES
- LOGIN PORTALS

```
almaz-antey.ru/robots.txt
www.almaz-antey.ru/robots.txt

User-Agent: *
Allow: /
Disallow: /bitrix/
Disallow: /local/
Host: http://www.almaz-antey.ru
```

Bitrix SaaS

Авторизация - almaz-antey.ru X +

www.almaz-antey.ru/bitrix/admin/index.php#authorize

www.almaz-antey.ru

### Авторизация

Пожалуйста, авторизуйтесь

Логин

Пароль

☐ Запомнить меня на этом компьютере

[Забыли свой пароль?](#)

или войдите через

Битрикс24



# BREACH DATA ENUMERATION

APP.FLARE.IO

1	2024-07-25	2023_Jeroymerlin.ru ⓘ		@almazantey.ru	1SpNKemF3
2	2024-05-29	combolists ⓘ		almazantey.ru	saxavat57
3	2024-05-29	combolists ⓘ		almazantey.ru	almazantey
4	2024-05-09	combolists ⓘ		almazantey.ru	ltqy2016
5	2023-04-13	2023_mars_combolists ⓘ		almazantey.ru	ltqy2016
6	2022-11-15	2022_november_combolists ⓘ		almazantey.ru	ltqy2016
7	2022-09-07	2022_START.ru ⓘ		@almazantey.ru	\$1\$sFIVAic>
8	2022-02-17	2022_january_combolists ⓘ		almazantey.ru	zgqmfezY
9	2022-02-17	2022_january_combolists ⓘ		almazantey.ru	zgqmfez
10	2022-02-17	2022_january_combolists ⓘ		almazantey.ru	almazantey
11	2021-12-11	2021_combolists ⓘ		almazantey.ru	saxavat57



# STEALER LOG DATA

Username

Password

Session Cookies (sites,discord,etc)

URLs to internal and sensitive sites

- Build attack flow from this data

Host information

- Processes running
- Browsers and versions used

# ATTACK SURFACE ENUMERATION

1. PORT SCANNING
2. SERVICE ENUMERATION
3. WEB CONTENT SEARCH AND DIRECTORY FUZZING
4. IDENTIFY INGRESS POINTS
5. CLOUD SERVICE DISCOVERY
6. RESEARCH UNKNOWN/UNFAMILIAR TECHNOLOGY STACKS
7. USER ENUMERATION
8. SUPPLY CHAIN LINKS

# ATTACK SURFACE ENUMERATION: PORT SCANNING

1. DON'T SCAN FROM YOUR LOCATION WITHOUT PROXIES.
2. DO SCAN FROM FRIENDLY-TO-TARGET COUNTRIES.
3. AS MUCH INFO AS POSSIBLE, FULL PORTS, SERVICE DETECTION, NMAP SCRIPTS FOR LOW-HANGING-FRUIT.

# ATTACK SURFACE ENUMERATION: SERVICE ENUMERATION

## 1. WITH NMAP SCRIPTS

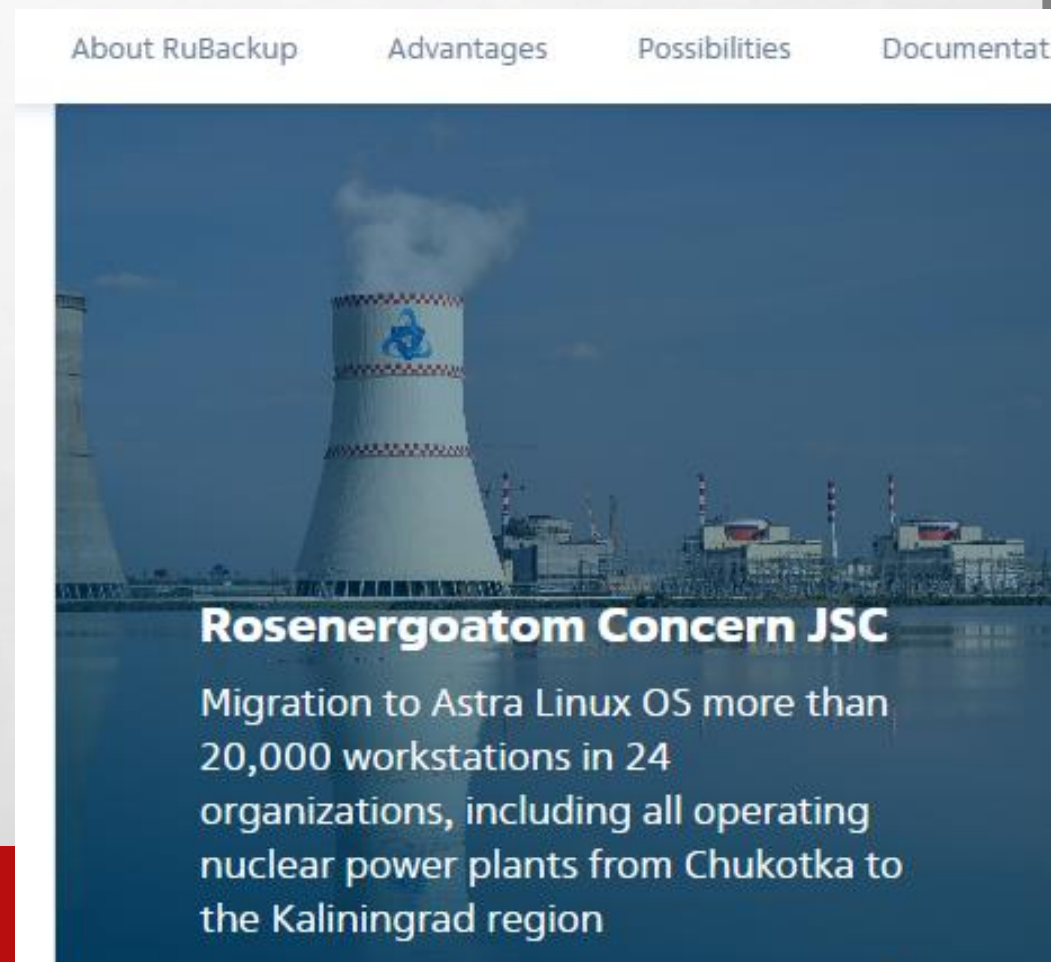
1.--SV --SCRIPT RMI-VULN-CLASSLOADER

2.--SV --SCRIPT SSL-ENUM

3.--SV NTLM-ENUM

# ATTACK SURFACE ENUMERATION: WESTERN TECH CLONES

1. ASTRAOS (SECURE DEBIAN)
2. ALDPRO (ACTIVE DIRECTORY)
3. TERMIDESK (TEAMVIEWER)
4. RUPOST (EMAIL)
5. BREST(VIRTUALIZATION)
6. RUBACKUP (BACKUP)





# UNFAMILIAR TECH: ACQUISITION

- POTENTIAL ACQUISITION ROUTES
  - PURCHASE IT.
    - LEGITIMATELY
    - ILLEGITIMATELY
  - THIEF IT.
  - FIND IT.

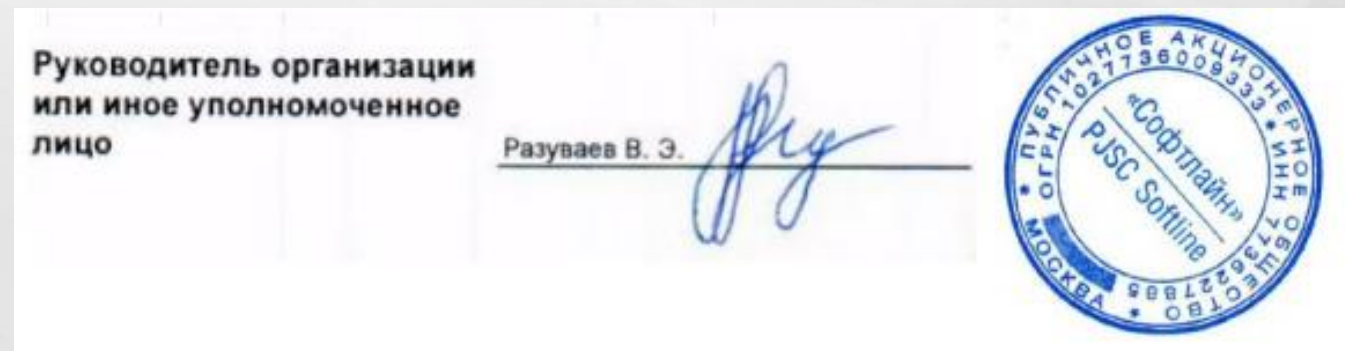
# STORY TIME: THE TALE OF SOFTLINE.RU

Goal: Attempt to purchase AstraOS Special Edition from Softline.ru.

Target: Softline.ru

- Identified HTTP code injection to list all buyers of the Special OS, including their required TIN and PoC email for registration.

Ruse: Create doppelganger @skiff.com email address for the .RU defense buyer, provide “stolen” TIN, get purchase approved. Success!



Legal entity and IP

Physical face

Details ?

Company

Legal address

TIN

checkpoint

Actual address

Delivery method

Email Delivery

February 22nd to the post office

Comment on order

Payment methods

Bank payment ?

Bank card ?

PLACE AN ORDER

Cart

Contacts

Delivery and payment

Legal entity and IP

Physical face

Details ?

Company

Legal address

TIN

checkpoint

Actual address

Delivery method

Email Delivery

February 22nd to the post office

Comment on order

Payment methods

Bank payment ?

Bank card ?

Заказ S00000000000000000000 принят

SS Softline Store B2B-маркетплейс <sales@softline.com>  
To: 00000000000000000000@skiff.com

ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.  
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

🌐 Translate message to: English Translation preferences

⏏ Right-click or tap and hold  
to download this picture.

Успешная трансформация. Цифровая. Защищенная.

Здравствуйтесь, Фтодосьев!

Благодарим вас за оформление заказа в интернет-магазине Softline!

Заказу присвоен номер S00000000000000000000 от 04.02.2024.

Состав заказа

Доставка: клин на E-mail  
Astra Linux Special Edition, x86-64, «Максимальный» («Смоленск»), ФСТЭК, способ передачи электронный, для рабочей станции, сроком на 12 мес., с включенными обновлениями Тип 2 на 12 мес.

1 шт. 28 700 руб.  
НДС не облагается

Итого 28 700 руб.

Оплатить заказ

№: 4028061240 КПП: 402801001  
Buyer: TIN: 4028061240, KPP: 402801001  
Name of the Buyer: ALMAZ-ANTAI GROUP LLC Address of the Buyer: Kaluga, ul. 1-ya Zagorodnaya, d 2  
Tel: +7 (849) 523-20-06

2. List of goods and rights to use computer programs provided to the Buyer under this Invoice (offer agreement):

No	Item	Name of Goods / rights to use a computer program	Packs*	Price, rub. RF	Amount, rub. RF	VAT, rubles. RF
1	OS2101X8617DI G000WS02-PO12	Computer program rights Special purpose operating system license appointments Astra Linux Special Edition for 64-bit platform based on processor architecture x86-64 (next update 1.7), security level Maximum (Smolensk), RUSB.10015-01 (FSTEC), method of transmission electronic, for updates for 12 months, with Type 2 updates included for 12 months	1	28 700,00	28 700,00	VAT is not taxable**

SUCCESS!




# Licenses and certificates

Software Licenses    Certificates for those. support    Certificates for updates    Service Certificates    Certificates for training

Product: Ald Pro    Certification: All    Architecture: x86\_64

Status: All    Start date: Select date    End Date: Select date    Table export

 Enter a search query

	License number	Name	Type	Qo	Start	Ending	Status
	207000010-ald-1.0-client-0-16234	Ald Pro	Workstation	2	12/28/2022	No time limit	Valid
	207000010-ald-1.0-client-0-16236	Ald Pro	Workstation	455	12/28/2022	No time limit	Valid



# ASTRAOS OVERVIEW



ECOSYSTEM OF RUSSIAN VERSIONS OF WESTERN SOFTWARE.

# ASTRAOS

- DESIGNED FOR SECURE NETWORKS.
- DEBIAN-BASED.
- VARIOUS LEVELS OF HARDENED SOFTWARE AND KERNELS.
- SMOLENSK UTILIZES THE HIGHEST LEVEL OF HARDENING AND IS TYPICALLY ONE MAJOR VERSION BEHIND WITH THE KERNEL.

*Select security level depending on the purchased license:*

Maximum security level Smolensk

Advanced security level Voronezh

Base security level Orel

Special Edition (Paid) - Provides advanced security features..

Spoiler: The Advanced security features

Mandatory access control,  
Modules isolation,  
Clearing RAM and external memory- Secure file deletion,  
Document marking,  
event logging,  
Information Protection procedures in graphics subsystem,  
User activity constraint mode (KIOSK MODE),  
protection of addressing space of processes,

ASTRA LINUX

ОПЕРАЦИОННАЯ  
СИСТЕМА

#### Additional OS settings

You can setup security settings depending on the selected mode, disable automatic network settings and setup system clock.

Additional OS settings options:

- ☒ Enable Mandatory Integrity Control
- ☒ Enable Mandatory Access Control
- ☐ Enable ELF signature check
- ☐ Clearing freed external memory
- ☐ Disable bootloader menu show up
- ☒ Disable ptrace capability
- ☒ Request password for sudo command
- ☐ Disable non-execution bit setup
- ☐ Enable scripts lock
- ☐ Enable macros lock
- ☐ Enable console lock
- ☐ Enable system limits
- ☐ Disable automatic network configuration
- ☐ Local time for system clock

# ASTRAOS: SECURITY FEATURES

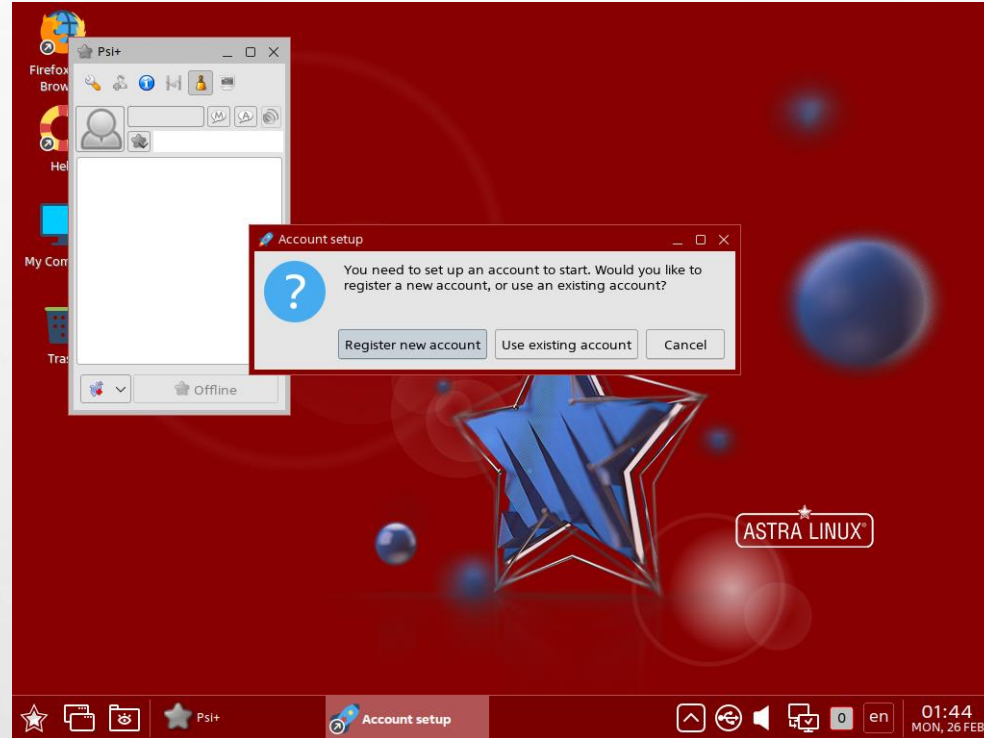




# ASTRAOS: DEFAULTS

## Hardcoded Parameters:

- Domain:ASTRA.LOCAL
- Users:Admin/Zabbix
- SSH saltuser/qwerty\$4



# SMOLENSK: FIRST-BOOT

BACKGROUND SWITCHES TO RED





**Software selection**

At the moment, only the core of the system is installed. To tune the system to your needs, you can choose to install one or more of the following predefined collections of software.

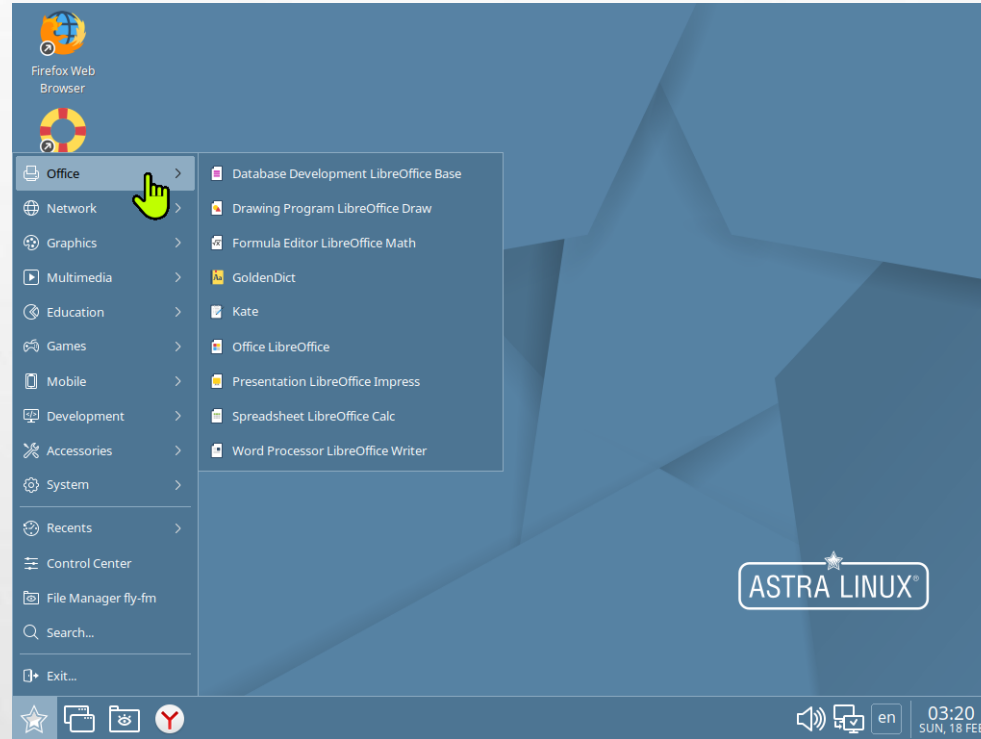
*Choose software to install:*

- ☒ Fly desktop
- ☒ Internet suite
- ☐ Office suite
- ☐ Graphics tools
- ☐ Multimedia
- ☒ Virtualization tools
- ☐ Games
- ☒ Base packages
- ☒ Ufw firewall
- ☐ Fly apps for working on devices with touchscreen
- ☒ SSH server

Screenshot

Help

Continue



# ASTRAOS FLY: FAMILIAR INTERFACE



# ALDPRO OVERVIEW



ACTIVE DIRECTORY-ISH

# ALDPRO:OVERVIEW

- [HTTPS://WWW.ALDPRO.RU/](https://www.aldpro.ru/)
- [HTTPS://WWW.ALDPRO.RU/DOCS/MANUAL/ALDPRO-DC-INSTALLATION-MANUAL-EN.PDF](https://www.aldpro.ru/docs/manual/aldpro-dc-installation-manual-en.pdf)

Meet **ALD Pro 3.0** :  
even more powerful, reliable, and convenient



The infographic is set against a dark blue background with a subtle pattern of stars and dots. It features several icons: a cube with a dollar sign and a gear for '30 ролей', a cube with an upward arrow for 'в 10 раз выше', a cube with a checkmark for 'Rapid implementation', a cube with a checkmark for 'Scalability', a cube with a checkmark for 'Multivendor', and a cube with a checkmark for 'Flexible policies'. A large blue box on the right contains the 'Built-in ACM' section.

**30 ролей**  
предустановлены в системе для более гибкого администрирования

**в 10 раз выше**  
производительность системы относительно релизов ALD Pro ниже версии 2.1

**Rapid implementation**  
ALD Pro Graphical Deployment Utilities

**Scalability**  
Reliable operation of DDO – the ability for Windows users to work in a Linux infrastructure, and vice versa

**Multivendor**  
Integrating a PC running Windows, RED OS, and Alt OS into the ALD Pro domain

**Flexible policies**  
The limit on the number of policies applied to a single computer or server has been removed.

**Built-in ACM**  
APM and Server Inventory Tool

- Hardware inventory
- Inventory of installed software
- Astra Linux License Management



# ATTACK SURFACE ENUMERATION: IDENTIFY INGRESS POINTS

## 1. KEY THINGS TO IDENTIFY:

1. RDP

2. VMWARE

3. VPN PORTALS HTTP(S)

1. WHAT TCP/UDP PORTS?

2. DOWNLOAD CONFIGURATION WITH VALID CREDENTIALS

4. VDI

1. CITRIX, ETC.



# ATTACK SURFACE ENUMERATION: CLOUD SERVICE DISCOVERY

## 1. YANDEX CLOUD

1. MARKET SHARE?

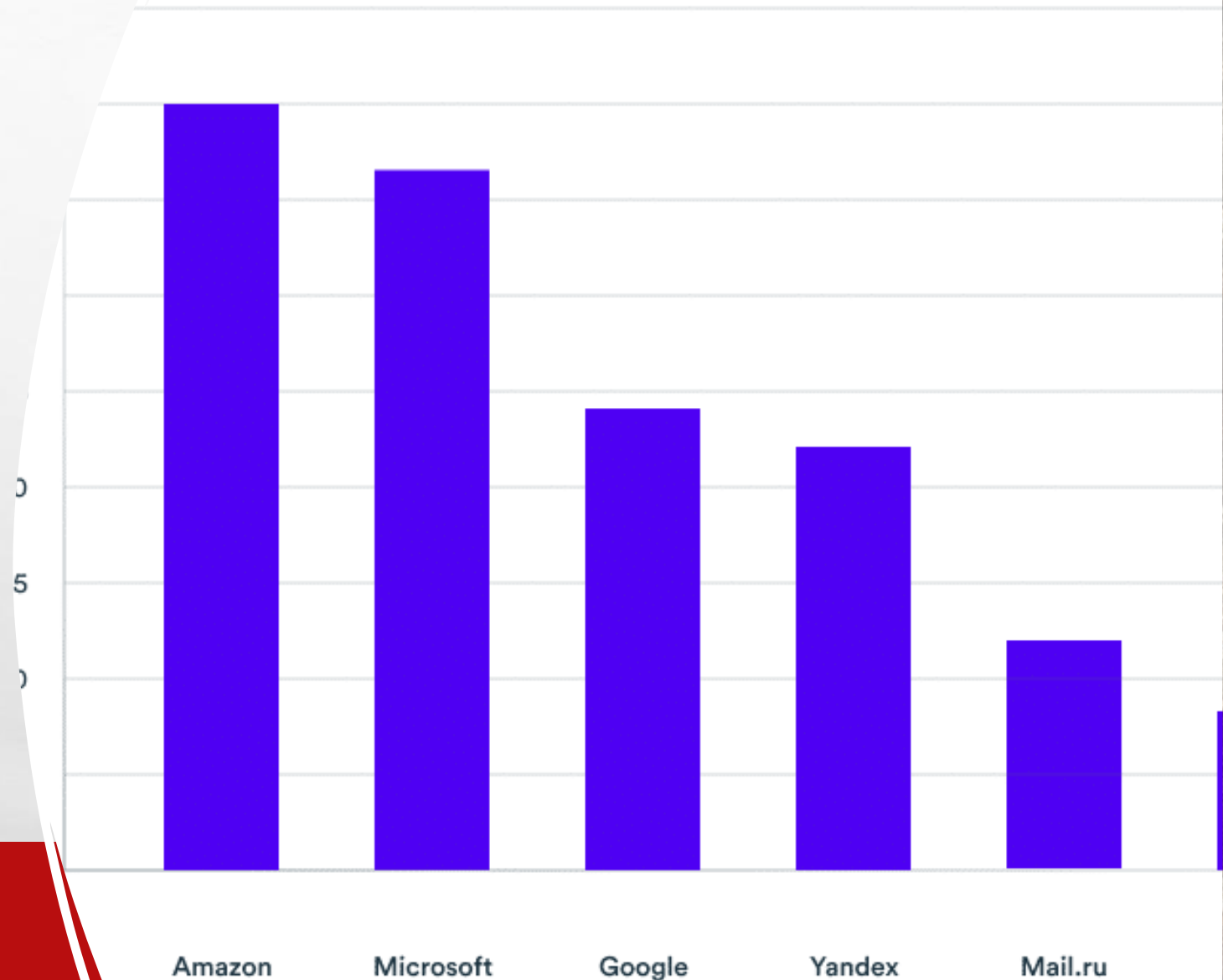
2. OFFENSIVE-USEFUL SERVICES?

1. COMPUTE

2. OBJECT STORAGE

3. CDN

<https://incountry.com/blog/global-clouds-and-cloud-providers-in-russia/>



# SQUEEGEE

- GATHER USERNAMES FOR FURTHER CREDENTIAL ATTACKS.
  - LOCAL ACCOUNT BRUTE FORCE
  - VPN PASSWORD SPRAY

```
[+] - Filename: 185.106.117.45.
[-] OS: Windows 7
[-] Patched: True
[-] Domain: None found
[-] Usernames:
    Andrievskaja
    Ejisk
    Korban
    Nadja
    Oksana
    Sushko
    USRICV33
    Администратср
    Пользсватель
    Гссть
```

# SQUEEGEE

- TWO-PART TOOL.
  - EXTRACT.PY
    - EXTRACTS RDP SCREENSHOTS FROM SHODAN OUTPUT
    - PYTHON3 RDPExtract.py -F 43DC50E7-DCEA-4F7D-A691-799E767E931D.JSON.GZ -D ~/DESKTOP/OP\_DATA/
  - SQUEEGEE.PY
    - USES OCR TO EXTRACT POTENTIAL USERNAMES FROM RDP SCREENSHOTS
    - PYTHON3 SQUEEGEE.PY -F ~/DESKTOP/OP\_DATA/ --LOG
- [HTTPS://WWW.BLACKHILLSINFOSEC.COM/INTRODUCING-SQUEEGEE-THE-MICROSOFT-WINDOWS-RDP-SCRAPING-UTILITY/](https://www.blackhillsinfosec.com/introducing-squeegEE-the-microsoft-windows-rdp-scraping-utility/)

# CREDENTIAL ATTACKS

1. USE THE USERNAMES CAPTURED FROM SQUEEGEE
  1. PASSWORD SPRAY SERVICES.
  2. BRUTE FORCING LOCAL WINDOWS ACCOUNTS USING RDP.
2. WORDLISTS
  1. LATIN OR CYRILLIC CHARACTERS?
    1. [HTTPS://GITHUB.COM/OOAFa/OOAFaSECLISTS/TREE/MAIN/PASSWORDS](https://github.com/OOAFa/OOAFaSECLISTS/tree/main/passwords)

# SOCIAL ENGINEERING

Language barriers make both verbal and non-verbal communications difficult. Russia is a large country with many regional dialects, your chances for success are low without proper translation assistance.



TL;DR avoid it, for now, cough, cough \*AI\*



# EXTERNAL SERVICE WEAKNESSES

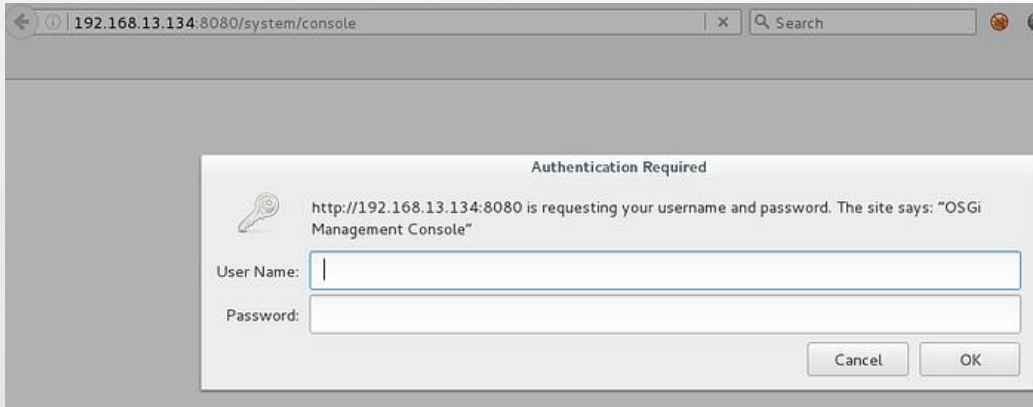
## 1.OVERVIEW

- 1.N-DAY ATTACKS.
- 2.JAVA DESERIALIZATION ABOUND, IF YOU LOOK.
- 3.EXCELLENT PLACES TO HIDE, YET COHABITATION CHECKS REQUIRED.

## 2.INDUSTRY STATISTICS

- 1.[HTTPS://WWW.PICUSSECURITY.COM/RESOURCE/BLOG/JANUARY-2024-KEY-THREAT-ACTORS-MALWARE-AND-EXPLOITED-VULNERABILITIES](https://www.picussecurity.com/resource/blog/january-2024-key-threat-actors-malware-and-exploited-vulnerabilities)

- [HTTPS://POSTS.SPECTEROPS.IO/SHELLING-APACHE-FELIX-WITH-JAVA-BUNDLES-2450D3A099A](https://posts.specterops.io/shelling-apache-felix-with-java-bundles-2450d3a099a)



# OSGI MANAGEMENT CONSOLE

192.168.13.134:8080/system/console/bundles

## Apache Felix Web Console Bundles

Main OSGi Status Web Console

Bundle information: 12 bundles in total - all 12 bundles active

x Apply Filter Filter All		
Id		Name
0	▶	System Bundle ( <i>org.apache.felix.framework</i> )
3	▶	Apache Felix Bundle Repository ( <i>org.apache.felix.bundlerepository</i> )
9	▶	Apache Felix Configuration Admin Service ( <i>org.apache.felix.configadmin</i> )
7	▶	Apache Felix EventAdmin ( <i>org.apache.felix.eventadmin</i> )
4	▶	Apache Felix Gogo Command ( <i>org.apache.felix.gogo.command</i> )
5	▶	Apache Felix Gogo JLine Shell ( <i>org.apache.felix.gogo.jline</i> )

# SHELLING APACHE FELIX

- [HTTPS://POSTS.SPECTEROPS  
.IO/SHELLING-APACHE-  
FELIX-WITH-JAVA-BUNDLES-  
2450D3A099A](https://posts.specterops.io/shelling-apache-felix-with-java-bundles-2450d3a099a)

# EXPLOITATION

1. IF IT MAKES SENSE.

2. YOU'RE MAYBE NOT THE FIRST.

1. COHABITATION PROTOCOLS.

3. DEFENSES

1. FIREWALLS: REDIRECTING THE WINDOWS FIREWALL MAY BE REQUIRED. 445 <-> 12445, AS AN EXAMPLE.

2. DISABLE THEM OR RESTRICT NETWORK ACCESS FOR THOSE PROCESSES.

# FIREWALL “BENDING”

```
netsh interface portproxy add  
v4tov4 listenport=31337  
listenaddress=0.0.0.0  
connectport=445  
connectaddress=127.0.0.1
```

```
netsh interface portproxy add  
v4tov4 listenport=31337  
listenaddress=0.0.0.0  
connectport=445  
connectaddress=10.10.100.20
```



# PAYLOADS

## 1. PAYLOADS

1. WHATEVER WORKS.

2. HANDLE THE DEFENSES PRIOR TO EXECUTION.

3. MISATTRIBUTION?

4. CHANNEL?

1. HOW ABOUT A WIREGUARD SERVER?

2. ASYNCHRONOUS/SYNCHRONOUS

3. THIRD-PARTY CHANNELS

4. SSH (BACKDOOR AUTHORIZED\_KEYS)

5. RDP

# COMPROMISING THIRD-PARTIES



## **Supply chain infiltration**

Check sanctions.



**Using compromised infrastructure  
or services as your own.**



**Partners and service providers.**

# POST-EXPLOITATION



# ACTIONS ON CONTACT

What might we need to do to move forward toward the overall objective from our initial exploitation point?



OODA at every step along the way.



Overview

Host Enumeration

Network Enumeration

Hash Cracking

Persistence

Lateral Movement

# COHABITATION CHECKS

- LIKELIHOOD OF ANOTHER ACTOR ON TARGET?
- [HTTPS://GITHUB.COM/OCTOBERFEST7/COHAB](https://github.com/Octoberfest7/COHAB)  
[PROCESSES](#)

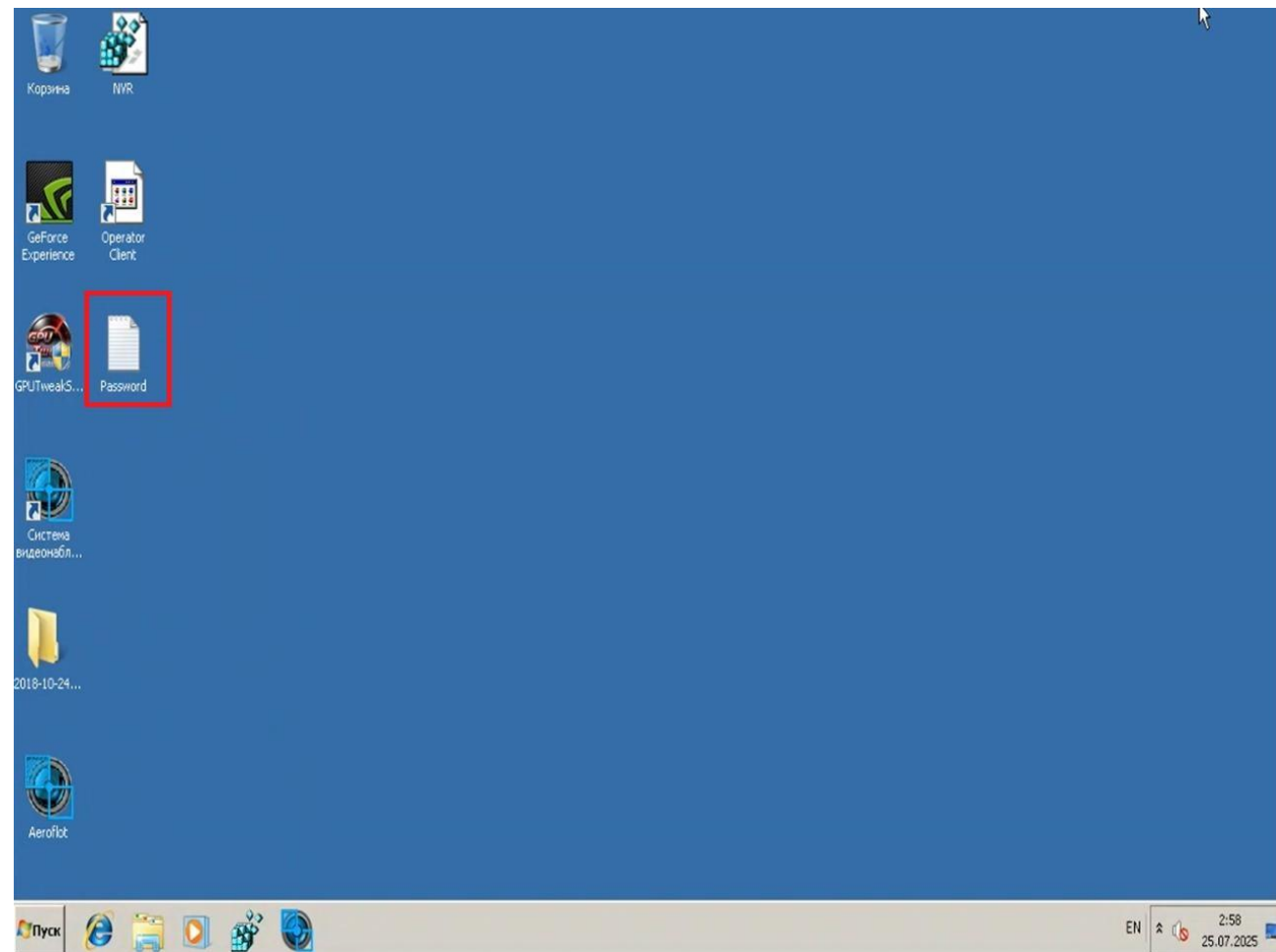




# HOST ENUMERATION

- IDENTIFY:
  - USERS.
  - PROCESSES/SOFTWARE.
  - INFORMATION PRESENT ON THE INITIAL ACCESS HOST.
  - CONNECTIONS TO OTHER HOSTS OR NETWORKS.

# AEROFLOT





# AEROFLOT ENUM



# NETWORK ENUMERATION

- IDENTIFY PROTOCOLS TRAVERSING DOMAIN.
- PROTOCOL ATTACKS WITHIN THE ASTRA ECOSYSTEM.
  - SAME? DIFFERENT?
  - LDAP(S), NTLM, KERBEROS, SMB, ETC.
  - RESEARCHING OTHER RU EQUIVALENTS AND ABILITIES/LIMITATIONS OF TOOLING.

# HASH CRACKING

## Common Hash Types

- NTLM mode 1000

## Russian Specific Hash Types

## Defined in Russian national standard GOST R 34.x

- GOST mode 6900
- Streebog modes 11700 (256), 11800 (512)

```
astra:$gost12512hash$Kk1.Aq/X$4j0E1Cv.IE1xKkgLfy71NpNMu  
9gf2E6jrnnsWx7VTGA1:19787:0:99999:7:::
```



# HASH CRACKING

- WORDLISTS
  - DO YOU “KNOW” WHAT LANGUAGE THE TARGET IS USING? EACH USER?
  - HAVE WORDLIST FOR ENGLISH AND RUSSIAN.
  - [HTTPS://RAW.GITHUBUSERCONTENT.COM/KKRYPTON/WORDLISTS/MAIN/WORDLISTS/LANGUAGES/RUSSIAN.TXT](https://raw.githubusercontent.com/kkrypt0n/wordlists/main/wordlists/languages/russian.txt)
- RULES
  - DO THEY WORK?
- TOOLS
  - [HTTPS://GITHUB.COM/RVRSH3LL/HASHCAT-NTLM-CYRILLIC](https://github.com/rvrsh3ll/hashcat-ntlm-cyrillic)

# LATERAL MOVEMENT



Internal to internal



Internal to cloud



Cloud to internal

# PROTOCOLS AND METHODS

- SSH
- SMB
- WMI
- WINRM
- RPC
- REMOTE DESKTOP
- SCCM/JAMF (WINDOWS/MAC)

# WRAPPING IT UP

- PROVIDE DELIVERABLES
- AFTER ACTION REVIEW (AAR)
- OPERATOR CLEAN-UP
  - NUKE ARTIFACTS
  - DON'T REUSE ANYTHING (UNLESS?)
  - MISATTRIBUTION AND PR
    - LEAKS/PLANTS
    - STATEMENTS

# THANK YOU!

[contact@futuresec.io](mailto:contact@futuresec.io)

[Medium.com/@rvrsh3ll](https://medium.com/@rvrsh3ll)

<https://www.blackhillsinfosec.com/category/author/steve-borosh/>

[github.com/OOAFA](https://github.com/OOAFA)