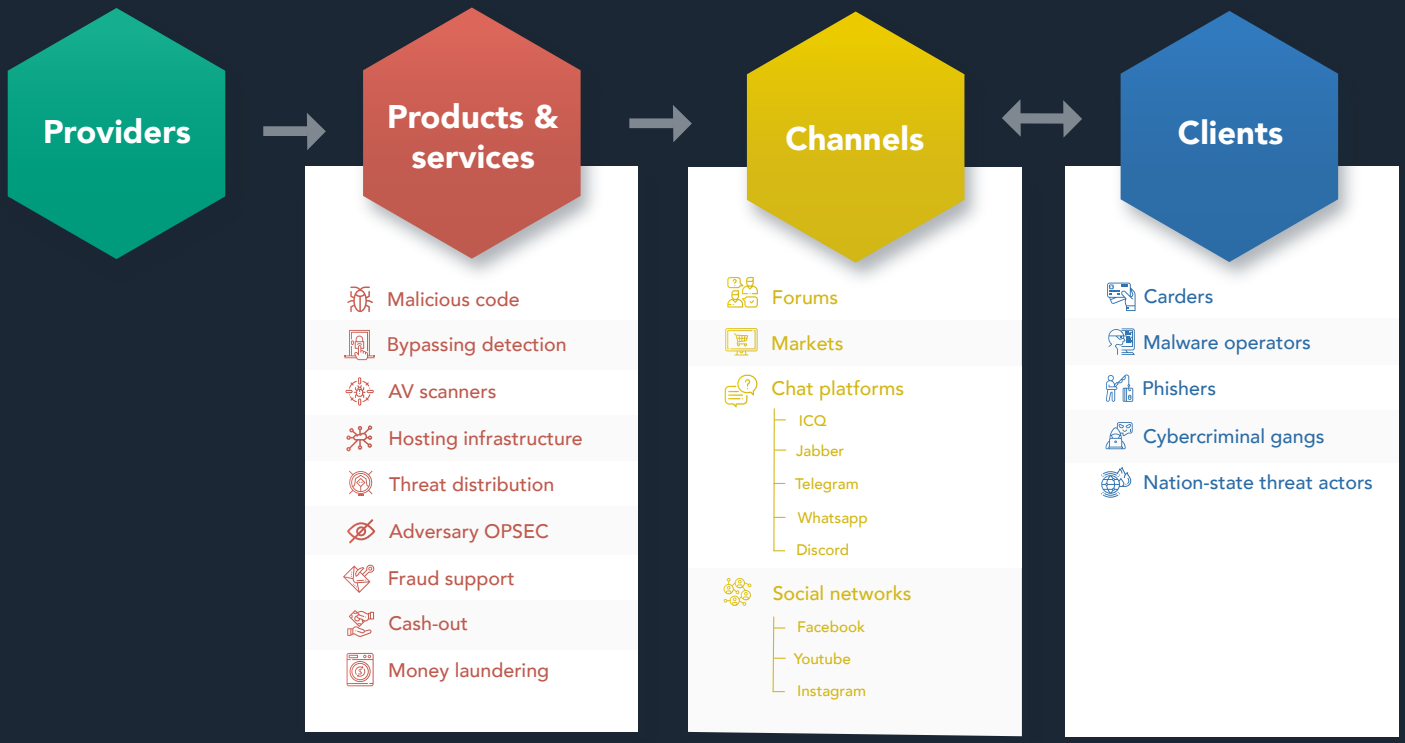
Blueliv.

EXECUTIVE SUMMARY

Cybercrime is an industry, with a growing service economy, tools for hire, service providers, channels and end users



The size of this shadow economy is growing. Cybercriminals of different levels of experience can acquire the necessary tools to launch a malicious campaign designed to attack businesses, governments and individuals

Understanding how attackers use these tools and services helps organizations prepare defenses and protect their assets

Build complete threat actor profiles

Analyze trends and patterns across different services utilized

Defend against targeted attacks

The first report in this series covers the first elements of this industry:
acquiring malicious code and preparing it for a campaign

HOW CYBERCRIMINALS OBTAIN MALWARE

Writing your own code

Ownership throughout entire campaign

Opportunity to learn from other actors

Labor-intensive

Specific skill sets required

Actors involved in operations as well as development

Hiring developers

Consultancy services can provide outside knowledge from other actors

Tailormade code designed to specifications

Expensive

High level of interaction required between vendors and clients

Hidden fees to keep projects private

Malware-as-a-Service (MaaS)

Easy to find, diverse and ready-to-use products

Little technical knowledge required

Cannot modify or alter code

Sometimes already detectable by AV engines

Blueliv.

MOST POPULAR MALWARE AVAILABLE

Prices of malicious code increase depending on the objectives, target operating systems, functionality, and version of the malware

Discounts available on some types of malware for splitting the gains of using it between users and developers

Some developers charge for 'add-ons' including additional modules, admin panel installation, privacy etc.

Prominent in Russian-language forums

VIDAR	$200-300 USD per month	$200-300 USD per month	Raccon Stealer
KPOT	$65 USD + add-ons	$150 USD + add-ons	Predator The Thief
Inter	$990 USD + discounts for splitting gains	Minimum cost of hiring a malware developer (Dr.Predator)	$80

UNDERGROUND COMMUNICATION

- Jabber / XMPP
- Discord
- Marketplaces
- Forums
- Telegram

Blueliv.

EVADING AND BYPASSING DETECTION

There has been a rise in the popularity of malware that includes a range of obfuscation, sandbox detection and bypass techniques

Most frequently used tools and services across malware types

Packers

Compresses malicious executables

Crypters

Encrypts malicious executables

PUBLIC

- Free
- Open licensed
- Often already 'known' to AV

PRIVATE (one-off)

- $100-300 USD
- Unique or custom
- Fully undetectable crypters

PRIVATE (subscription)

- $30 – 90 USD per month
- Constantly evolving
- Fully undetectable crypters

Obfuscator

Obscures, conceals, or disguises source code

Many are legitimate tools

Varying price ranges from $50 – 3000 USD though some are free

Cheapest based on quota of files requiring obfuscation

Most expensive usually carry a subscription and software license

Code signing

Applications that carry an official signature to confirm integrity of the application; identify author of the code

Three types of vendors:

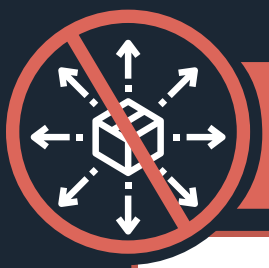
- Resellers
- Intermediary managers
- Binary certification services

Legitimate certificates priced between $500 - 3000 USD

Blueliv.

TESTING ANTIVIRUS AND BLACKLIST EVASION

Finalized malware products and infrastructure must be tested before deployment



No distribute antivirus scanners

Users can test files, URLs, domains, and IP addresses against security protections without distributing elements they scan to security vendors

Static scans test malware across AV products and generate reports

Dynamic scans additionally deploy the malware and provide runtime analysis

Make changes to infrastructure

Tweak products before launch

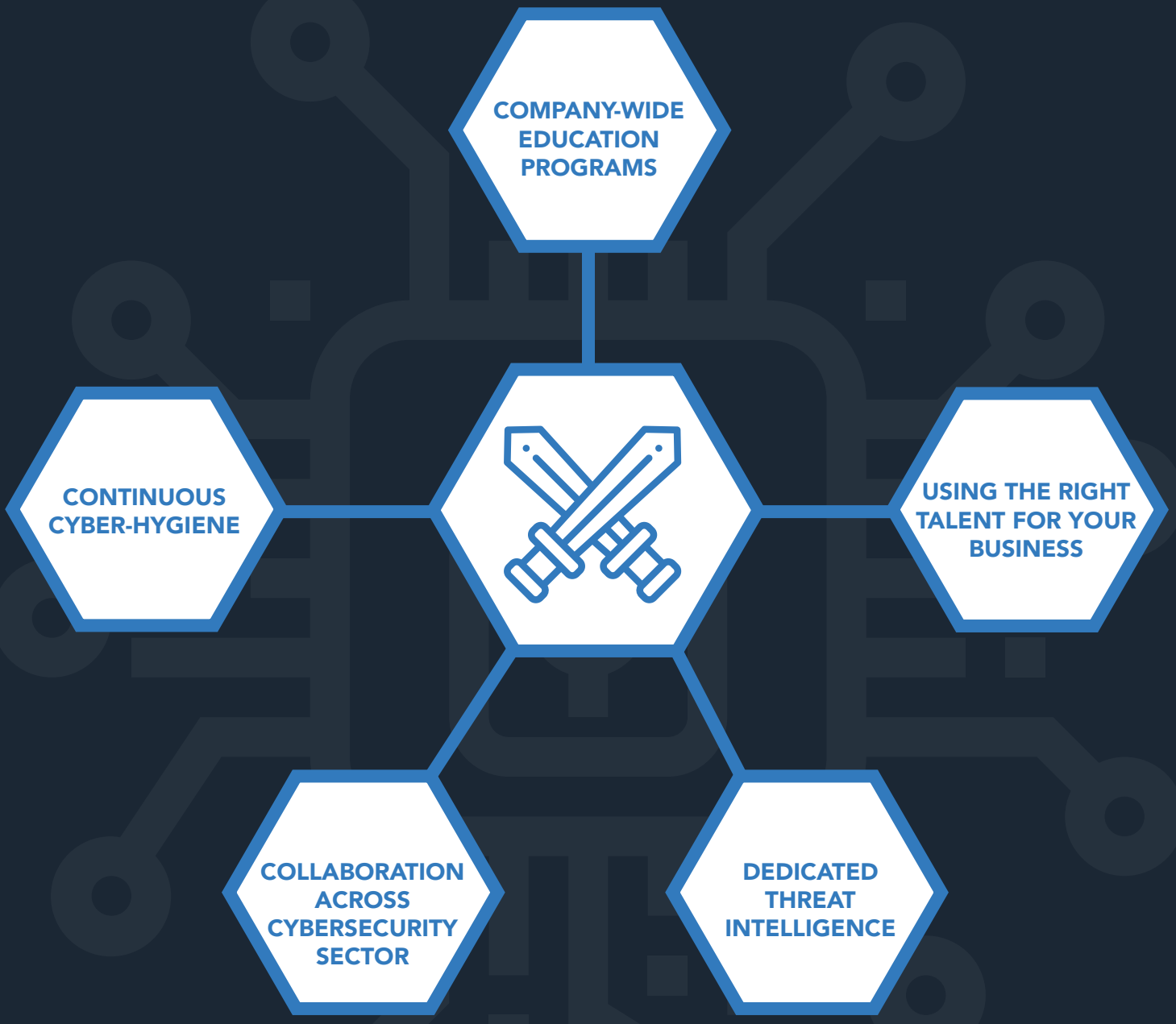
Improve stealth of tooling

Free models, seemingly supported by paid advertising

Single-scan pricing from $0.01 USD depending on provider

Subscription-based models range from $50 to $299 USD per month

CONFRONTING THE CYBERCRIMINAL INDUSTRY



Blueliv hosts the Threat Exchange Network to aid collaboration.
Join the fight against cybercrime today.

community.blueliv.com