

Access-as-a-Service – Remote Access Markets in the Cybercrime Underground

 ke-la.com/access-as-a-service-remote-access-markets-in-the-cybercrime-underground/

May 13, 2020

Bottom Line Up Front

Remote Access Markets are automated stores that allow attackers to exchange access credentials to compromised websites and services. As such, **they represent an endless stream of opportunities for attackers**; buying access to an organization as a service lowers the skill bar for further exploitation and exposes organizations to a plethora wave of online threats – from ransomware to card skimming.

This blog will review one prominent Remote Access Market out of the several tracked and monitored by KELA – MagBo. This store is unique in a few different aspects, but mostly in volume of goods: over two years of operations, **it featured access to nearly 150,000 compromised websites – including financial institutions, government organizations and critical infrastructure around the world** – mostly via selling access to web shell malware deployed on their servers. KELA advocated that gaining visibility into MagBo, as well as other Remote Access Markets, is a crucial intelligence feed for defenders.

Background

Like any other industry, the cybercrime sector is also exploring innovative business models, adopting technological tools to improve monetization opportunities. In an effort to transform cybercrime into a more scalable, lucrative business with a higher ROI, actors focus on several revenue-generating schemes.

Reviewing the current market, we can see two major trends:

1. Servitization – actors are gradually adopting a *Something-as-a-Service* model, instead of struggling to profit from tutorials, software or digital goods. This is noticeable in the prominence of Malware-as-a-Service (especially among ransomware providers), as well as other aspects of the cybercrime ecosystem.

2. Sales Automation – a few years ago, the best way to monetize a product or a service was posting in a forum and waiting for buyers. Nowadays, cybercriminals are leaning heavily into *Autoshops*: automated click-to-buy markets that allow a buyer to purchase goods or services without relying on cumbersome human intervention, boosting sales volumes and making business more scalable.

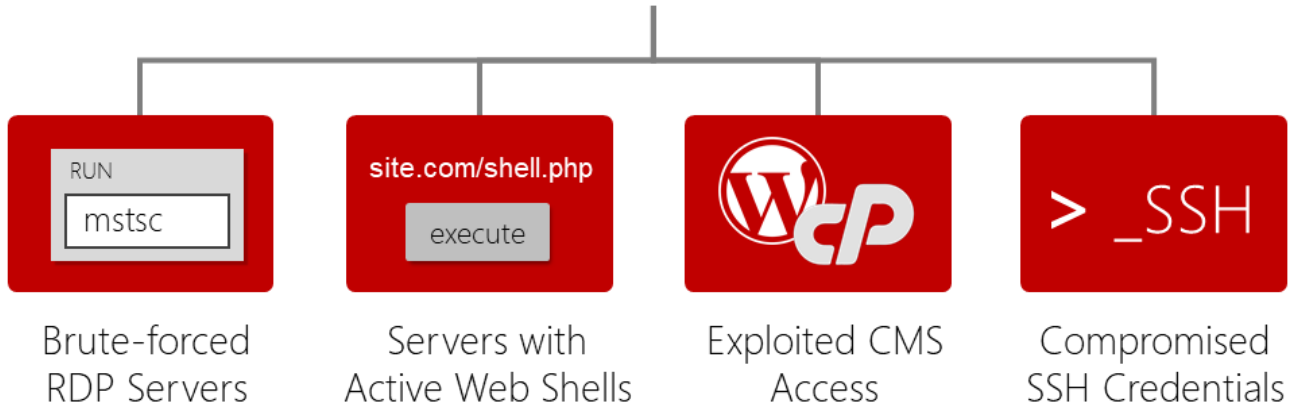
These have always been popular practices when it comes to the obvious deliverables of cybercrime: **Account shops** like [Slilpp](#) have been peddling millions of brute-forced accounts for years; and up until a couple of months ago, [Deer.io was a major player](#) enabling threat actors to quickly and easily set up dedicated autoshops. Lately, however, more and more actors and groups have been investing in autoshops selling more advanced goods; one example is the [Genesis Store](#) and the MaaS business model it features, allowing easy monetization of botnet infections.

Remote Access Markets

A prime example of the more sophisticated actors in the autoshop field are what KELA refers to as **Remote Access Markets – stores offering access to compromised servers and websites**. The [xDedic RDP store](#), an infamous market that operated until authorities shut it down in 2019, was a one-stop-shop for breached servers accessible via Remote Desktop Connection protocol, where attackers could buy credentials and immediately gain access to compromised servers. The concept of easily buying remote access can be very appealing to a wide variety of attackers: **from ransomware operators trying to gain foothold within a corporate network to APT actors looking for silent entry point to a target organization**, these markets provide excellent opportunities.

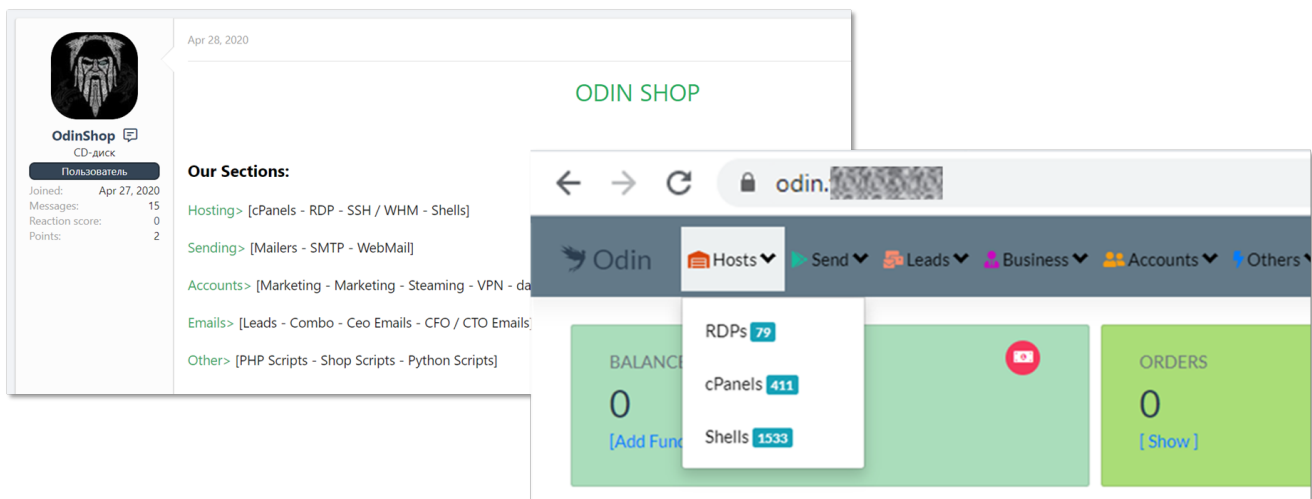
Remote Access, however, can be obtained in various ways – not just over RDP. Threat actors are able to abuse content management systems, SSH, etc. to gain access to a network asset for multiple use cases – anything from manipulating the content of a website hosted on the server to using it as infrastructure for further operations within the corporate network.

REMOTE ACCESS MARKETS



Several cybercrime shops and vendors sell different Remote Access products – with a varying level of product quality. Some threat actors offer Remote Access credentials; others operate RDP-dedicated autoshops while some use forums to post transactions of web shell batches.

Just last month, a new player, named Odin Shop, launched a store selling several Remote Access items (dubbed “hosting” or “hosts”) among other wares, such as consumer account and email lists. The shop has three sections dedicated to remote access – RDP servers, website administration panels and web shells – each catering to a different attacker use case.



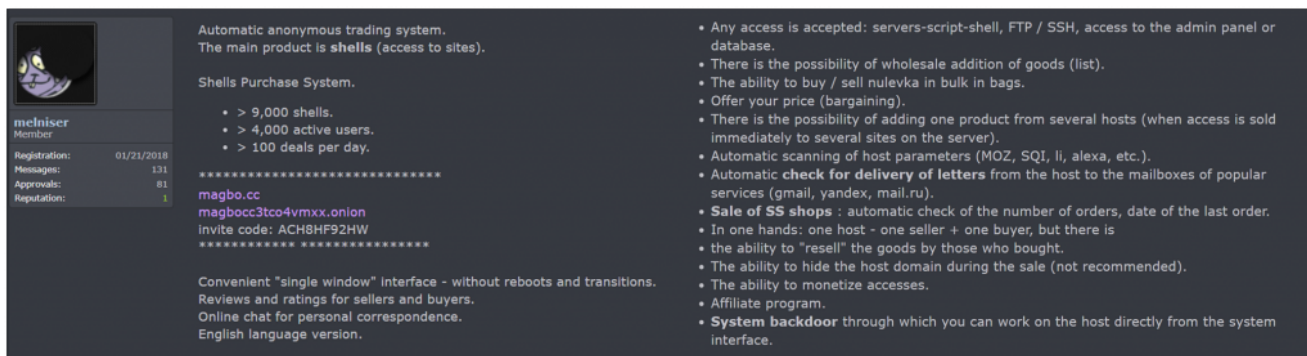
Promoting the Odin Shop on Russian hacking forum (left); and a preview of the shop (right)

A new actor, Odin's reputation and credibility have yet to be determined by cybercrime communities; it's possible that trying to be a one-stop-shop, instead of specializing only in remote access, would compromise its product quality.

On the other end of the spectrum lie several stores that specialize only in remote access, with most of them tailoring to one specific access niche. Within these niches operate shops that specialize in RDP access, SSH credentials and more. This blog will focus on one store of interest out of the several Remote Access Market monitored by KELA – **MagBo, a highly-vetted and reputable autoshop specializing in web shells.**

It's All About the Access

MagBo is an invite-only automated market for diverse products specializing in Remote Access credentials, and specifically in web shells.



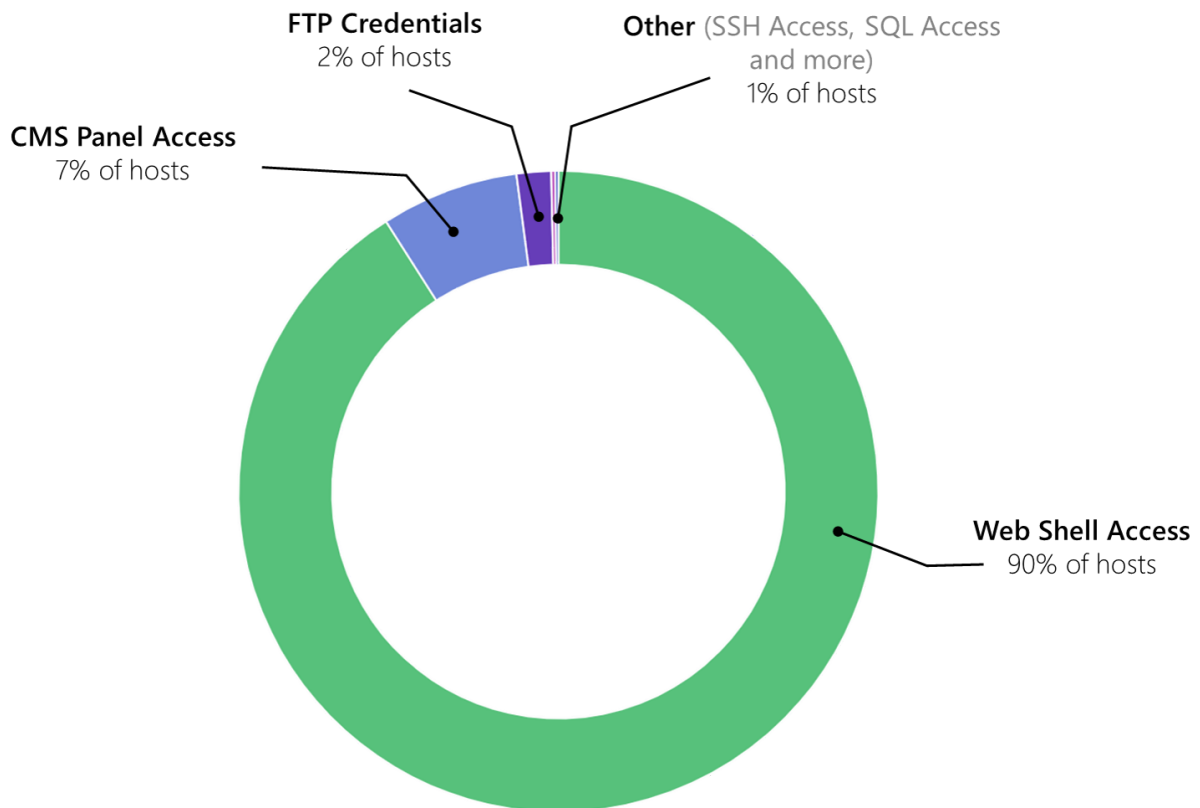
The screenshot displays the MagBo website interface. On the left, there is a user profile for 'melniser', a member since 01/21/2018, with 131 messages, 81 approvals, and a reputation of 1. The main content area is titled 'Automatic anonymous trading system. The main product is shells (access to sites).' and 'Shells Purchase System.' It lists several statistics: '> 9,000 shells.', '> 4,000 active users.', and '> 100 deals per day.' Below this, there is an invite code 'ACH8HF92HW' and a list of features. The features include: 'Any access is accepted: servers-script-shell, FTP / SSH, access to the admin panel or database.', 'There is the possibility of wholesale addition of goods (list).', 'The ability to buy / sell nulevka in bulk in bags.', 'Offer your price (bargaining).', 'There is the possibility of adding one product from several hosts (when access is sold immediately to several sites on the server).', 'Automatic scanning of host parameters (MOZ, SQI, li, alexa, etc.).', 'Automatic check for delivery of letters from the host to the mailboxes of popular services (gmail, yandex, mail.ru).', 'Sale of SS shops : automatic check of the number of orders, date of the last order.', 'In one hands: one host - one seller + one buyer, but there is the ability to "resell" the goods by those who bought.', 'The ability to hide the host domain during the sale (not recommended).', 'The ability to monetize accesses.', 'Affiliate program.', and 'System backdoor through which you can work on the host directly from the system interface.'

MagBo's launch post on a Russian forum

Officially launched in early 2018, MagBo has been not only evolving but also growing in volume and variety. Initial reports cited it sells “over 3,000 breached websites”; **by late April 2020, it had over 28,000 servers totaling around \$700,000 worth of goods.** During our research, we were able to track 43,000 unique hostnames posted on MagBo for which we have full details; based on historical data, KELA is able to assess that **over time MagBo has offered almost 150,000 distinct compromised websites for sale.** These websites include anything from government offices and ministries sold for USD 10,000 a piece to small-business websites offered for a few cents.

These extensive numbers of compromised servers are mostly accessed via web shells – but not exclusively. True to its promise to support a wide variety of cybercriminal use cases, MagBo offers access via different means. Around 90% of the listings are web shells, while

7% and 2% offer Remote Access via compromised CMS and FTP credentials, respectively; the remaining 1% is comprised of a plethora of other access methods – from SSH to hosting admin panels.



Breakdown of remote access vectors offered on MagBo (May 2020; n = 43,000)

According to KELA's analysis, **between 200 and 400 new compromised servers are added to the market** on an average day – making it a fairly active market; **the number of daily transactions is around 200**, suggesting the market enjoys steady growth. One reason for this might be the operation model – MagBo is a decentralized platform serving multiple threat actors who can upload their wares. KELA's data shows **190 different threat actors currently have active listings on the market**.



MagBo by Numbers

Analysis by KELA Targeted Intelligence, May 2020



150,000

Compromised websites posted to since 2018



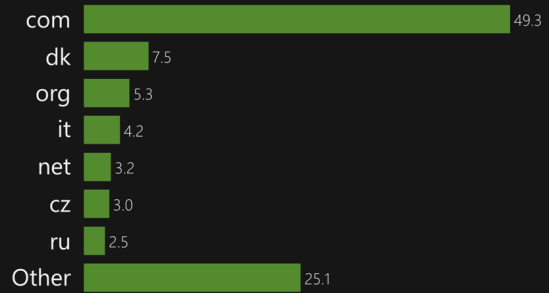
USD 750,000

Worth of goods offered as of May, 2020; n = 43,000



190

Threat actors currently selling accesses on market



Most popular top-level-domains of compromised websites featured on the market, by percentage

While the number of Remote Access items offered on MagBo definitely helps it stand out, it is only one of the *Killer Features* that attract cybercrime actors.


Killer Feature #1: Transparency of Goods

As cybercriminals become more sophisticated and develop more niche requirements, businesses catering to them must keep up. Compared to other sellers of Remote Access – specifically via web shells – **MagBo has a distinct advantage: it provides much more information that helps potential buyers evaluate the quality of product.**

Following are examples of two web shell vendors associated with Russian cybercrime communities – one selling access via forum posts, the other operating an autoshop. Neither provides buyers with useful information, like the full DNS of the compromised server, exact permissions or other metadata:

NightWwWolf Posted May 23, 2019 (edited) Report post ↗

megabyte
●●●



Paid registration
🔒 2
71 posts
Joined
05/13/19 (ID: 92830)
Activity
безопасность / security

Selling web shelves. Price 0.5 \$ pcs. Minimum purchase of 10 \$ I can shed your file. There is http and https. I can make shells for sib. Write - what you need - what I can do) jabber: nightwolf@jabber.cz or write to the PM - I often check

Edited May 23, 2019 by

+ Quote

Shells Market

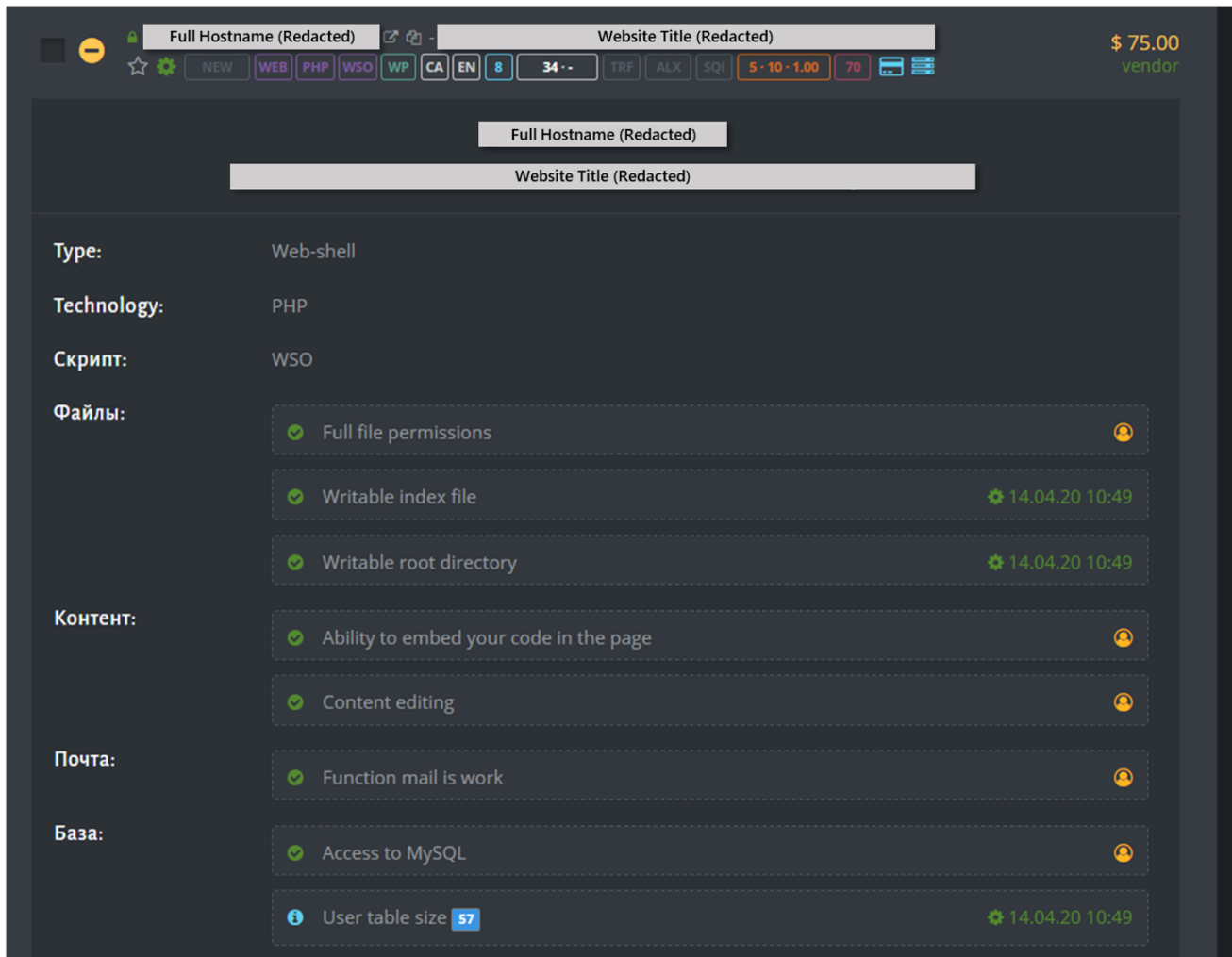
All shells are with **full rights** hosted on **root-level** domain

Show entries

#	Domain	Buy	Protocol	AlexaGlobal	AlexaCountry
7050	m*****s.com	10 \$	HTTP	NONE	NONE
6982	p*****x.com	10 \$	HTTP	NONE	NONE
6955	g*****d.com	10 \$	HTTP	NONE	NONE
6904	c*****p.com	10 \$	HTTP	NONE	NONE
6899	j*****f.com	10 \$	HTTP	NONE	NONE

Web Shell vendors offering goods missing essential details

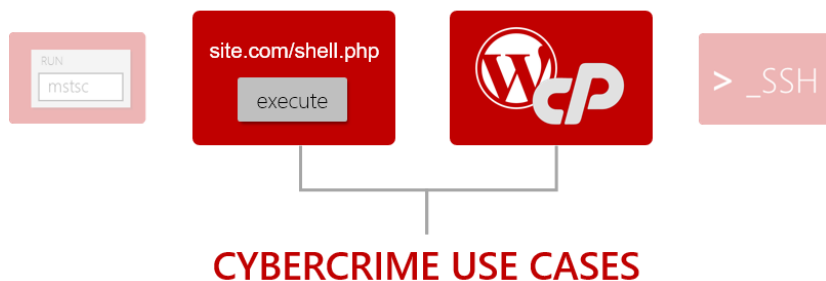
MagBo, on the other hand, **focuses on providing rich server details** – from the actual hostname down to the specific permissions an attacker could leverage. Below is a MagBo listing (identifying details redacted by KELA), showing the level of granularity the market provides:



Example of a MagBo listing with a detailed view of a compromised server

This detailed list serves not only malicious actors; it also allows defenders to understand the type of operations an attacker might execute on a compromised server. The listing above indicates, for example, the “function mail is work” – meaning, an attacker can use it to send phishing or spam emails; it also indicates that a malicious actor with access to the shell could embed code in the page, serving malicious content or sniffing traffic for credit card skimming as part of a Magecart attack.

MagBo



- Installing a card skimmer on a compromised website (Magecart)
- Altering the website to serve malicious content via an exploit kit
- Hosting commodity malware admin panels on website
- Abusing the website's mail server for spam or phishing
- Hijacking website content or external links for black-hat SEO

MagBo offerings by specific permissions and features

Based on forum posts made by the market's admin, maintaining this level of transparency is a crucial function of MagBo; in a message from January 2018, the admins mentioned an option to hide exact DNS names but advised against it:

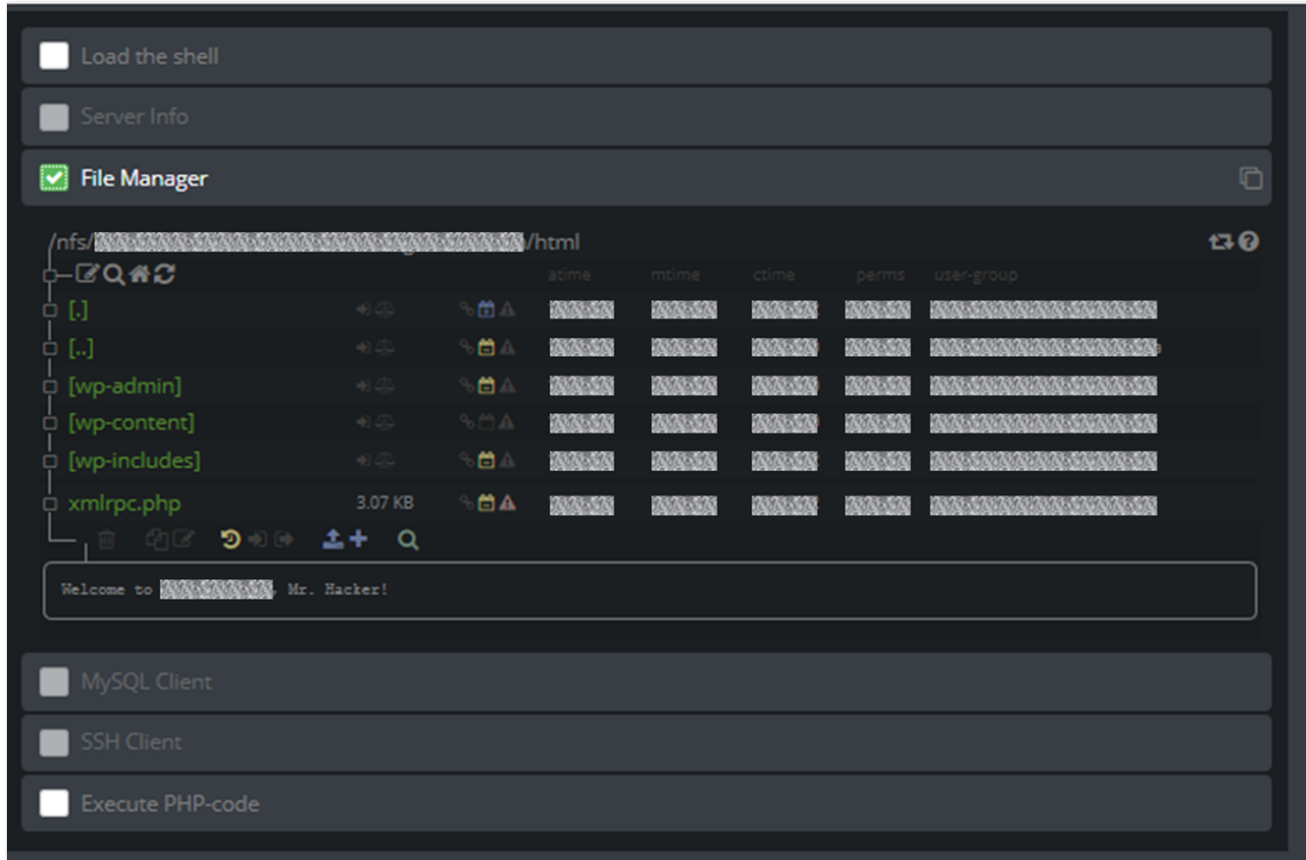
The screenshot shows a forum post by user 'melniser'. The post text reads: 'The ability to hide host domains has been made. However, this is strongly discouraged. Buyers lose the opportunity to see both the domain and title, screen and other info on the product. Domains are not hidden for buyers with purchases above 100.' Below the text is a reply from user 'navai' who says: 'as for convenience, I would argue. why it was impossible to take the service from the same baker, moreover, its owner offered to give it for free.'

MagBo admins advising users against applying the option to hide the full DNS of a compromised server

Killer Feature #2: MagBo Backdoor

Once an actor acquires remote access credentials to a compromised website, they can start working on the actual use case that would serve their purposes; this includes accessing the server and performing actions that would further exploit it. MagBo does more than just providing clients with login credentials – it supplies a backend platform that can be used to carry out the actual attack.

MagBo Backdoor (MBD) is a **second stage web shell** that interacts with the **MagBo website**. An attacker can install it on a compromised server to make the web shell more compatible with MagBo's business model. Once running, **MBD can be used to perform actions on the server from the MagBo UI**: loading malware, running arbitrary code via PHP and more.



Help → System Backdoor

Sellers can use a special system backdoor for placement on the sold sites. The advantages of this method of providing access is that the system itself collects information about the product, as well as transfers the goods to the buyer.

When using the system backdoor, the transaction is confirmed automatically immediately after purchase or after 3 hours. The system itself checks the availability and performance of the backdoor, as well as controls the transfer of goods to the buyer and confirms this fact. The opportunity to complain within 3 hours is related to counteracting a possible imitation of the backdoor by some potential fraudster.

Also, the system backdoor will work if the system recognized the seller's script (for example, WSO). In such cases, the system backdoor code is executed in the shell of a third-party script or loaded through it. No changes are made to the parent shell and no files are left.

Attention! The administration does not accept complaints about the operation of the system in the absence of a system backdoor on the site! In this case, you must contact the seller for restoration of access.

Backdoor description

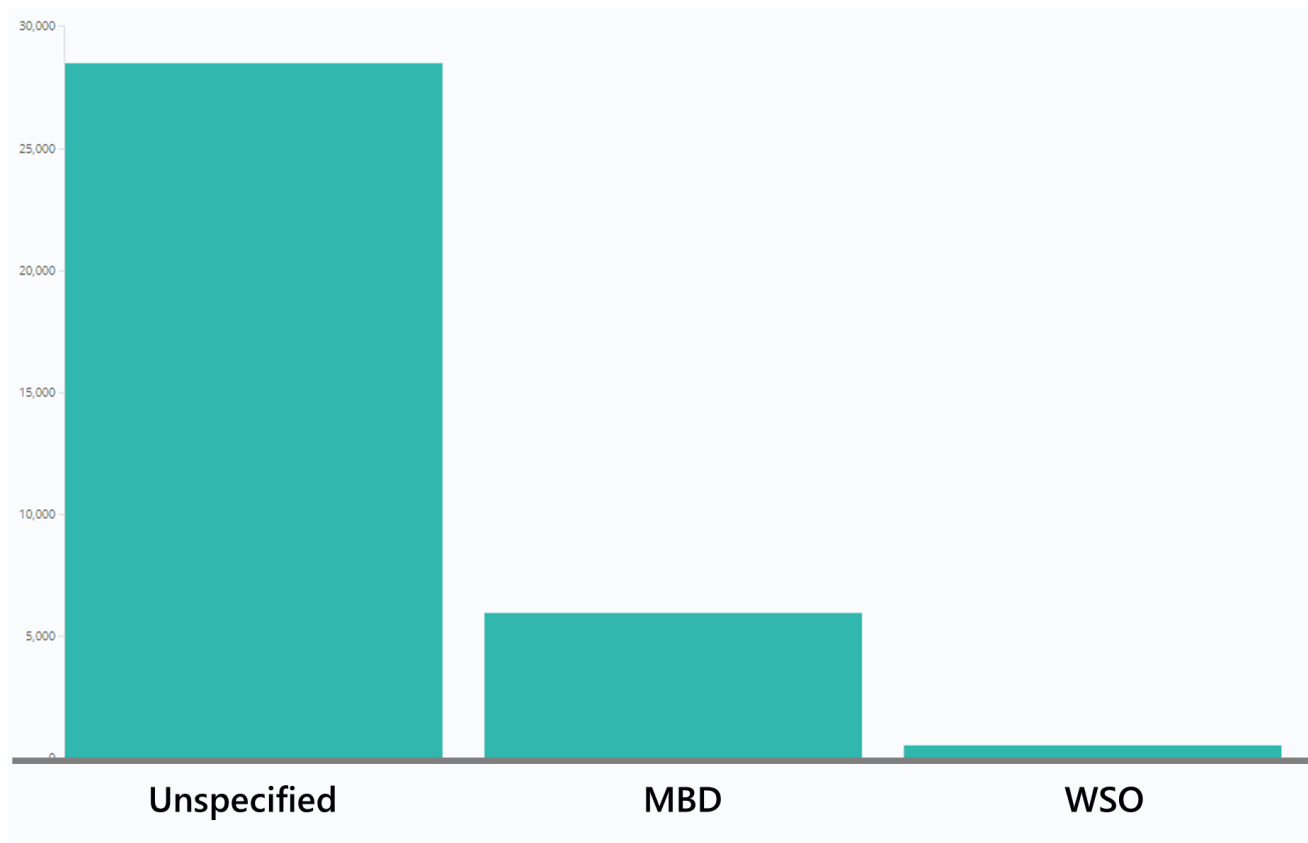
Access to the server is through the execution of functions from the array value. Additionally, the necessary module files are loaded, which are stored in the directory of temporary server files. The work takes into account the server software versions in order to minimize the number of errors and warnings in the logs and reduce the risk of detecting the backdoor.

The backdoor on the site interacts with the system through the API using a special key issued by the system for a specific session. The API can be accessed either directly or through a proxy site to hide request addresses from the admin server. All settings are automatically adjusted by the system.

The MBD UI featuring the file system of a compromised server (top); and a brief overview of MBD on MagBo's FAQ (bottom)

MBD suggests MagBo **aims to be a platform – a one-stop-shop for web shell access and management AND a technology provider**. In that sense, it carries on xDedic's legacy of helping clients optimize and maintain access to the servers sold on the market.

However, actors are slow to adopt MBD; based on data obtained by KELA, only around 6,000 web shells on the market utilized MBD in May 2020.



Breakdown of web shell types offered on MagBo

Remote Access Markets & the Enterprise Defender

Covering the basics of cybercrime threat intelligence – paste sites, traditional markets and forums – is crucial for any cybersecurity intelligence practitioner. However, we continue to advocate that tracking automated shops ensures defenders have a unique edge by **monitoring actual corporate assets**. The most basic use case here is obvious: **if a cybercrime market sells access credentials to any of your corporate network devices**, you'd *probably* want to be aware of that ASAP. In monitoring Remote Access Markets, KELA has found multiple instances in which our clients' assets – from esoteric domains used by subsidiaries up to major servers who are part of production environments – has been posted for sale on a market. **Our real-time monitoring and analyst-assisted escalation are crucial to remediate the threat in real time** and prevent attackers from further leveraging the access.

There is, however, much more that can be done with data obtained from Remote Access Markets. One example can be monitoring your vendors and supply chain, not only your own assets, to gain a better understanding of your threat landscape and third-party attacks surface. Another is consuming a list of compromised network assets as **high fidelity indicators of compromise**; obtaining real-time access to these data streams provides a supplementary IOCs feed featuring compromised domains. By consuming it directly from the source, you avoid waiting until after the fact, when a domain has been found to be malicious.

Whatever a defender chooses to do with Remote Access Markets data – and these examples are just the tip of the iceberg – KELA believes that retaining these feeds is invaluable.

Moreover, MagBo's apparent success and ongoing investment in technology suggests it's here to stay – and others are quickly joining: xDedic's takedown prompted the rise of other RDP markets that fill the vacuum while vendors specializing in monetizing SSH credentials are gaining traction. The trends of Servitization – **providing Access-as-a-Service** to be leveraged by actors – and automation are on the rise; it's safe to assume more cybercrime enterprises will enter these markets and expand operations.