



The Hacker Infrastructure and Underground Hosting: Services Used by Criminals

Vladimir Kropotov, Robert McArdle, and Fyodor Yarochkin

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Published by

Trend Micro Research

Written by

Vladimir Kropotov

Robert McArdle

Fyodor Yarochkin

Stock image used under license from

Shutterstock.com

For Raimund Genes (1963 – 2017)

Contents

4

Criminal Applications of
Underground Hosting

7

Current Underground
Infrastructure Services

38

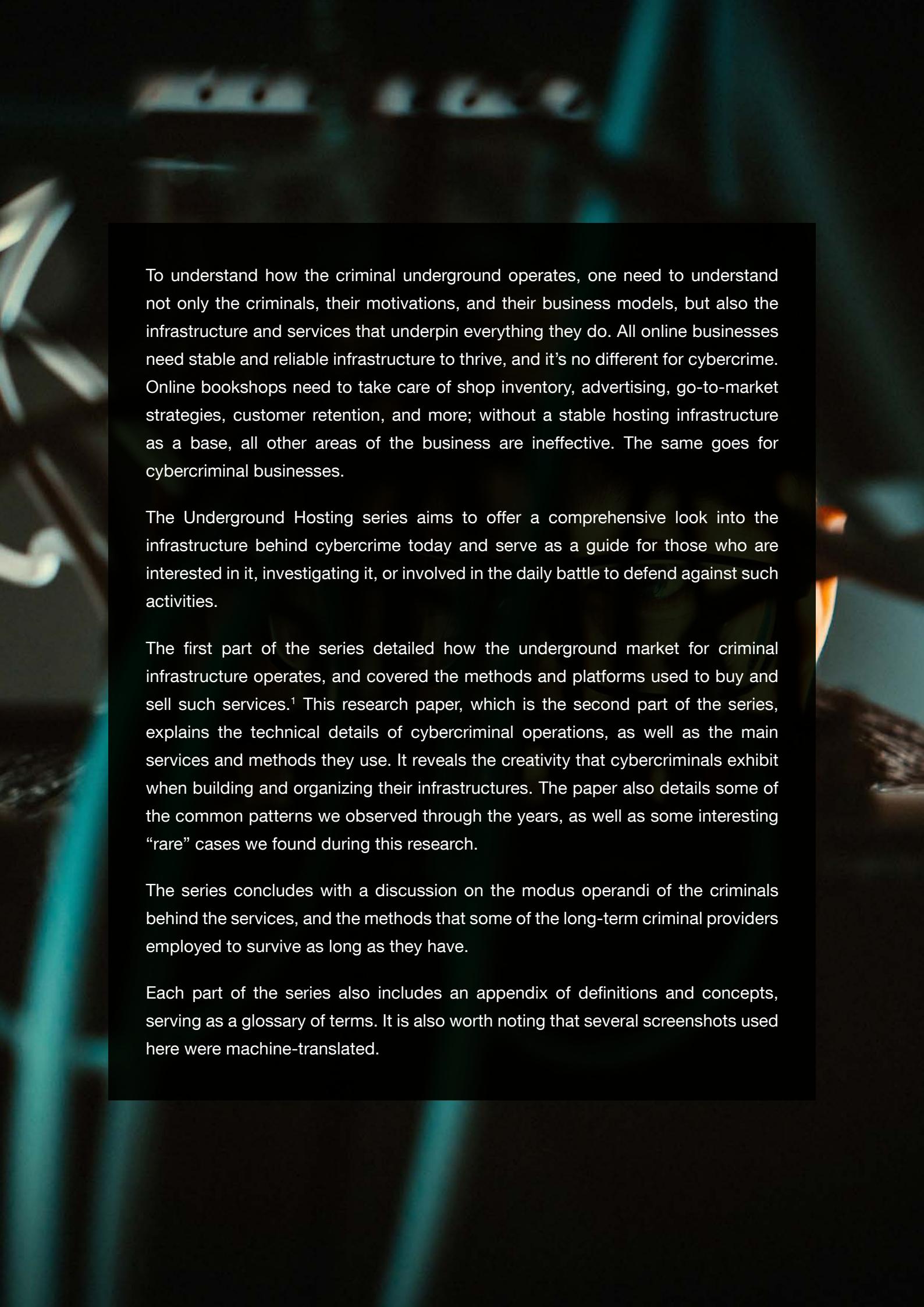
Emerging Trends in Underground
Infrastructure Services

49

Conclusion

50

Appendix



To understand how the criminal underground operates, one needs to understand not only the criminals, their motivations, and their business models, but also the infrastructure and services that underpin everything they do. All online businesses need stable and reliable infrastructure to thrive, and it's no different for cybercrime. Online bookshops need to take care of shop inventory, advertising, go-to-market strategies, customer retention, and more; without a stable hosting infrastructure as a base, all other areas of the business are ineffective. The same goes for cybercriminal businesses.

The Underground Hosting series aims to offer a comprehensive look into the infrastructure behind cybercrime today and serve as a guide for those who are interested in it, investigating it, or involved in the daily battle to defend against such activities.

The first part of the series detailed how the underground market for criminal infrastructure operates, and covered the methods and platforms used to buy and sell such services.¹ This research paper, which is the second part of the series, explains the technical details of cybercriminal operations, as well as the main services and methods they use. It reveals the creativity that cybercriminals exhibit when building and organizing their infrastructures. The paper also details some of the common patterns we observed through the years, as well as some interesting “rare” cases we found during this research.

The series concludes with a discussion on the modus operandi of the criminals behind the services, and the methods that some of the long-term criminal providers employed to survive as long as they have.

Each part of the series also includes an appendix of definitions and concepts, serving as a glossary of terms. It is also worth noting that several screenshots used here were machine-translated.

Criminal Applications of Underground Hosting

Network infrastructure is an essential component of any criminal enterprise, and many criminal groups have very specific requirements. Some simply need short-lived servers that could be used for network scanning or phishing email distribution, whereas others require solid bulletproof hosting that can run backend hacker infrastructure and would be hidden by a series of reverse proxies to make it more difficult for security researchers or law enforcement to identify.

So how do cybercriminals typically use underground and bulletproof hosting (BPH)? Underground hosting accommodates services that carry a variety of purposes from traffic direction systems (TDS) to host command and control (C&C) infrastructure.

Let us examine and review some of the most common cases:

- **Hosting of websites with illegal or questionable content**

Cybercriminals do host regular websites. These sites could be underground forums and online shopping platforms where cybercriminals sell digital assets and services such as credentials, credit card dumps, access to compromised systems, virtual private networks (VPNs), virtual private systems (VPSs), and BPH.

Cybercriminals also utilize the web hosting space to host phishing websites and doorway pages, which are frequently used for search engine optimization (SEO) activities and other purposes.

Where are these hosted? Resources such as compromised blogging platforms (such as WordPress) are often utilized for these purposes. We also observed attackers modifying the content of legitimate websites to serve specific content when search engine crawlers visit them.

- **Hosting of command and control infrastructure**

This is typically one of the “holy grail” components for many cybercriminals. C&C hosting may include platforms that host secondary malicious payloads downloaded by initial loaders, ransomware backends, and systems that are being used for data exfiltration and direct control of compromised machines. These systems are very important to the attackers, as the takedown of such systems could lead to a loss of data access. They can also provide clues to law enforcement if seized and examined by cyber forensic specialists.

Where are these hosted? Cybercriminals often apply additional measures to protect and conceal the location of such systems by using cloud services and hosting these platforms on darknet (.onion) sites or using a series of reverse proxies.

- **Hosting of service-provision components**

Many cybercriminal operations require additional components such as TDS platforms and exploit kit landing/forwarding pages. These pages often use disposable landing domains and front pages, and such front-end components are very short-lived. The takedown of such components does not have a significant impact on hacker operations because they are prepared for such scenarios and can readily migrate their infrastructure to new locations.

Where are these hosted? Cybercriminals are often comfortable with short-lived hosting platforms such as cloud and even legitimate compromised resources.

- **Hosting of anonymization and proxying/reverse proxying components**

Proxying and anonymization services are widely used to conceal cybercriminal tracks, hide the location of actual C&C systems, and anonymize attacker activities. However, because these services are also used for legitimate purposes such as bypassing internet censorship or preserving user privacy, many of the providers of such services operate in “gray” areas. They cannot be considered as services used for purely criminal purposes.

Where are these hosted? These are often legitimate hosting and service companies because the provision of these services is not illegal.

- **Platforms used for running internet scans and credential brute-force attacks**

These are often short-lived disposable systems that attackers continually use to acquire access to new systems. They are often hosted on legitimate but compromised systems so that attackers can collect their log data before abuse requests are sent and processed or addressed by the actual host.

Where are these hosted? Compromised systems or cloud-based VPS systems are often used for these purposes.

After such activities are conducted on these compromised systems, these systems would often appear in blacklists for blocking. These can become a nuisance for the owner of these systems or the internet service provider (ISP), considering that the ISP itself can be blacklisted.

- **Platforms used to conduct phishing and spam mail distribution**

Since many of the email systems often verify and validate email sending machines, many attackers seek newer systems to distribute spam and phishing mail. Legitimate email servers can also be compromised and/or exploited to distribute phishing and spammed content.

Where are these hosted? Threat actors can use end-user machines that have been compromised by a botnet component, or legitimate web services.

- **Participation in online fraud activities such as click fraud**

These systems often run mass web spamming software (like XRumer) and attacker tools that mimic user behavior and produce fraudulent web clicks on web advertisements and views on online media channels.

Where are these hosted? These systems are often hosted on disposable servers, either compromised or in a cloud infrastructure.

The abovementioned categories are generalized examples of cybercriminal applications that run on BPH platforms. Different hosting platforms can be tailored to be better suited for use in one or more of these applications.

Current Underground Infrastructure Services

For the reader's benefit, we decided to split the second paper of the series into three core sections. The first part will focus on the most common categories of underground infrastructure services that we observed being advertised and used by criminals today. We categorized these into the major overarching areas such as:

- Dedicated hosting services
- Compromised hosting services
- Privacy and anonymizing services
- Domain provisioning services

Depending on their business model, criminals use a mix of dedicated and compromised assets, along with robust domain provisioning — all through the use of a variety of anonymizing services to protect their privacy.

Our second section will then focus on emerging trends in underground infrastructure. These are not future trends, and instead, represent service that does not have the same volume of usage as those we have highlighted in our current section.

Finally, in a detailed appendix, we included a case study looking at the overall lifecycle of a compromised server that ties many of these services together, which we believe will be of value to asset owners.

Dedicated Bulletproof Hosting Services

We define underground hosting as any service provided to host components or infrastructure to conduct malicious and criminal activity. Within that definition, the subcategory of bulletproof hosting refers to hosting setups that are highly resistant to disruption and takedown — either through ignoring abuse requests or requests from international law enforcement — or through the technical aspects of their setup. This section details the major categories and trending methods used to accomplish this hosting, as well as the ways it is protected from rival criminal groups' attacks and law enforcement probing.

Dedicated and Virtual Private Servers

Dedicated and virtual private servers (VPS) are the core parts of many underground hosting services. These systems are used to host criminal infrastructure components — such as botnet control panels, phishing pages, and other elements — used in cyberattacks. Attackers can also use them as “jump servers” with static IP addresses to access other infrastructure securely. In doing so, attackers ensure their IP addresses are kept out of logs of their final targets. For such services, attackers have the main options available to them, as shown below:

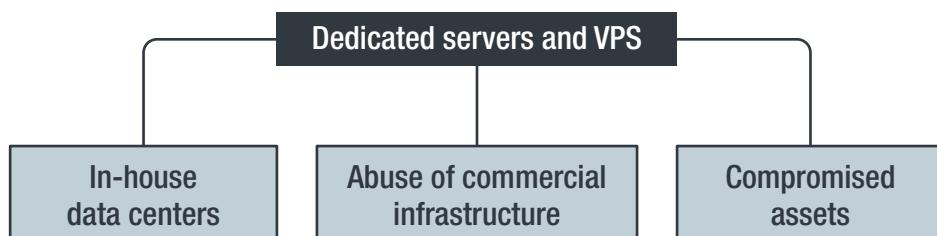


Figure 1. Types of dedicated servers and VPS available in the underground market

Criminals often use “in-house” infrastructure in countries where hosting such content is considered legitimate, or in countries whose legal frameworks are difficult to apply when dealing with cybercrime. In-house, in this case, refers to servers located in the private property of individuals or small groups offering it to threat actors, as opposed to larger commercial entities. This ranges from racks of servers in a side room of the house to individual hosting in certain places.

For example, we identified several hosts operating in Belize and Seychelles. We believe that the geographic locations of the hosting providers were chosen for a specific reason. Another example² of such infrastructure was hosted in Ukraine and could be seen below, which was uploaded on YouTube by the Security Service of Ukraine’s official channel.

The video shows over 100 servers taken down by the Security Service of Ukraine. These servers, which were located in a private house in the south of Ukraine, were sold in underground forums under nicknames “webhost,” “webhosting,” “whost,” and “AbdAllah.”

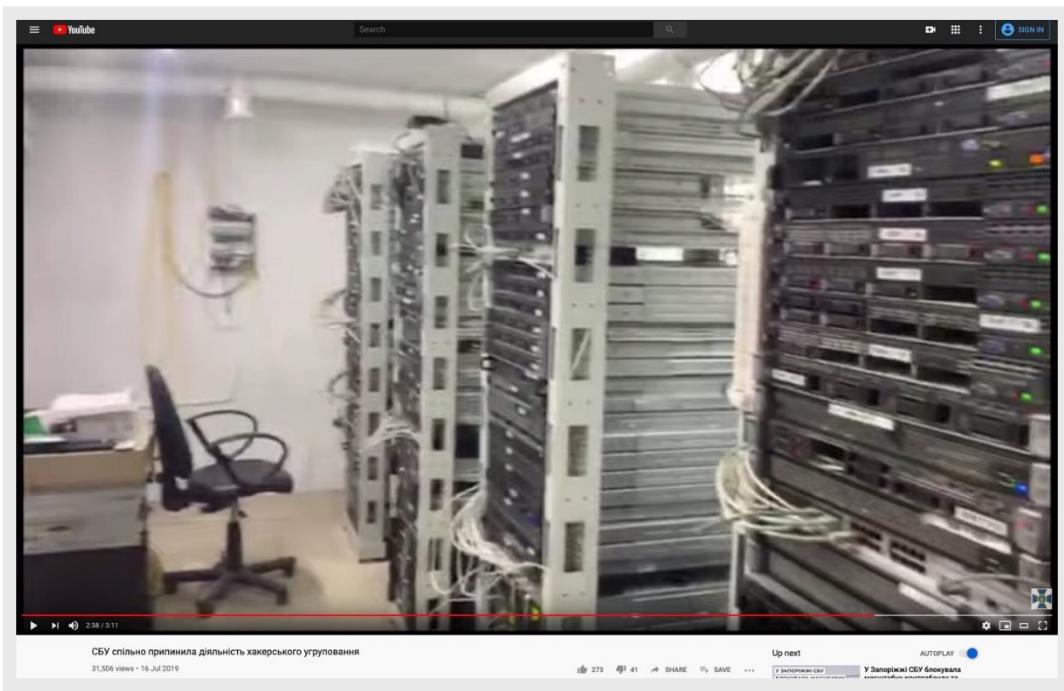


Figure 2. An in-house data center in Ukraine

Commercial infrastructures have tighter restrictions, and are typically used in two situations:

- To host services and content that are permitted in the country in which these servers are physically located.
- To host services or content that have a short lifespan. In these cases, the time to respond to abuse requests could be longer than the time for the underground actor's activity. A phishing campaign could be an example.

We discuss dedicated servers and VPS systems that use compromised machines later in this paper.

Modern Fast-Flux

Fast-flux is a technique used to ensure the availability of services through high-frequency switching of domain resolution to a pool of IP addresses. For a criminal, this provides increased resistance to takedown and disruption, as their server's location (or at least the path from a victim machine connected to it) is constantly changing, hence "in flux." This pool of IP addresses often acts as a reverse proxy, and could be supplied through multiple resources: rental of virtual machine instances from a cloud provider, botnet nodes, or compromised machines.

The core of the fast-flux technique is in using short TTLs (time-to-live) for domain name resolution caching, which prevents the domain name caching at intermediate resolvers and forces them to always request resolution from declared domain name system (DNS) servers. This short TTL caching allows attackers to perform high-frequency switching between IP addresses (the fast-flux IP pool) and ensuring that the service is available, even if certain IP addresses were taken down, reported, or blocked by an ISP.

Threat actors have been using fast-flux networks for quite some time. In modern fast-flux service offerings, we often see it used as an intermediate “high-availability” layer between the client and the actual server:

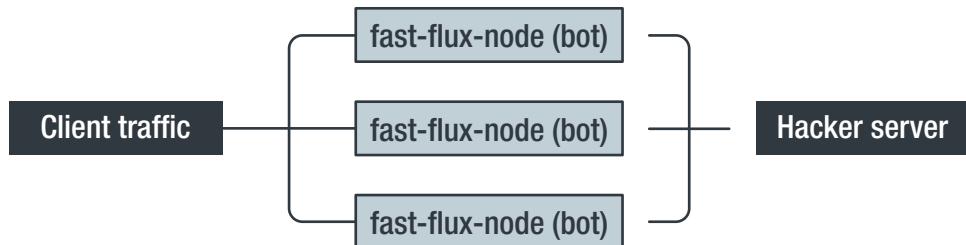


Figure 3: Typical use of fast-flux

The following screenshot from a forum demonstrates a typical fast-flux offering. The high-service availability is one of the most essential criteria of such a service, as the customer would normally lose information (and thus money) if the service becomes unavailable.

[E N G]

Our services will change your opinion about the servers.
([Hosting](#) * [VPS / VDS](#) * [Dedicated Servers](#) * [FastFlux](#) * [Domain Registration](#)).

+ *Loyal price policy / reasonable prices.*
+ *High UpTime 99.9%.*
+ *Individual approach to each client.*
+ *We work directly with the DC / server in the racks.*
+ *Our priorities are stability and speed.*

Figure 4. Fast-flux offering (often combined with dedicated servers and domains)

When examining domain names, short TTLs in SOA statements combined with the IP resolutions in many different autonomous system numbers (ASNs) is usually (but not always) a telling sign that a fast-flux infrastructure is providing the domain name. Let's look at this example:

```
XXXXXX.com. IN SOA a.{BLOCKED}d.com.  
domainadmin.{BLOCKED}d.com.  
1549401388; Serial, in this case is a unix timestamp  
3600; Refresh  
180; Retry (common value is 1800)  
1209600; Expire (common value is 604800)  
180; Minimum TTL (common value is 86400)
```

The values of TTLs shown in red are set with unusually low retry and minimum TTL times (in seconds). Under normal circumstances, this would create additional load on a DNS server; however, in the case of fast-flux, the objective is to suppress the caching mechanism of resolvers and let the client receive the IP address that is currently being provisioned by the fast-flux infrastructure. The DNS server, in turn, will need to regularly update its A records (IP resolutions) to the next batch of IP addresses in the fast-flux supply pool.

Use cases of fast-flux services vary. During our research, we saw fast-flux-based infrastructure being used in an exploit kit serving chain, hosting C&C IP addresses for call-home communication, and data exfiltration purposes by tools such as web credit card skimmers and mobile malware.

Fast-flux-backed services are normally more expensive to operate compared to other bulletproof hosting services, and the difference in pricing reflects this. After all, the operator needs to maintain a pool of IP addresses to provision fast-flux infrastructure, which comes at an additional cost. The following figure shows the difference in pricing (USD):

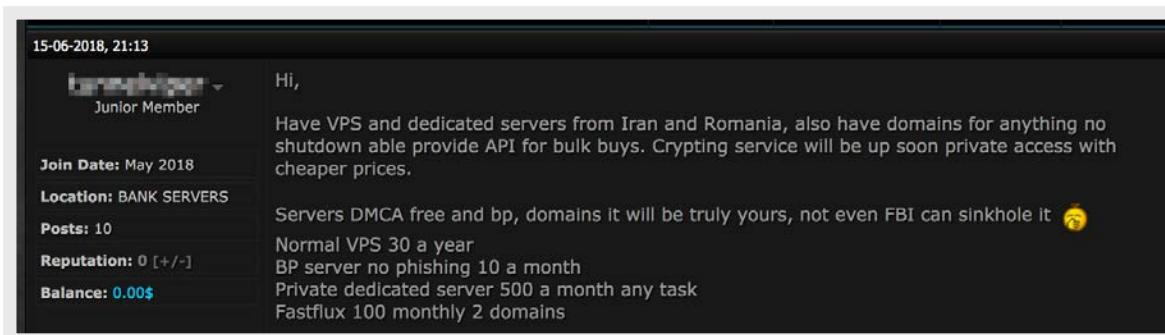


Figure 5. Cost comparisons in hosting services

There are several providers of fast flux-based infrastructure in the underground. Each of them provides its servers differently. For example, we observed that a provider often procures their infrastructure through a variety of cloud services, including Google Cloud, Microsoft Azure, and Alibaba Cloud.

DDoS Protection Services

Distributed denial-of-service (DDoS) protection is a popular service in the underground hosting market. While it may seem unusual, criminals need DDoS protection, just like legitimate companies. Just as organizations compete with each other, so do criminal groups. In their case, they have no problems with carrying out cyberattacks (like DDoS) to disrupt the competition.

Some bulletproof hosts list DDoS protection as one of their offerings. To help illustrate these offerings, we will examine one such bulletproof service provider. While we use one provider here to illustrate the sort of offerings found, these offerings are common among DDoS protection providers.

The bulletproof host we found on the surface web provides a wide range of services, from anonymous domain registration to SSL certification provision and bulletproof proxy. The bulletproof proxy appears to protect from both network-level DDoS attacks and application-level attacks through placing a web application firewall-like (WAF) control in front of the protected resource.

The same host provides a wide range of additional services, including Onion site (Tor) registration/hosting, webmail, and VPN. A full list of other available services can be seen below:

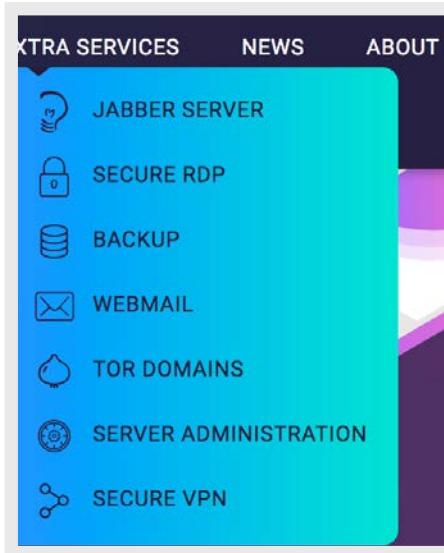


Figure 6: Other services from the bulletproof service provider

Interestingly enough, the IP range related to the provider is geo-located in Ukraine, while the organization is registered in Belize.

We believe that many of the bulletproof hosts prefer such countries as the place of registration because it's difficult for international law enforcement agencies to obtain timely information on systems and organizations located in those geographical regions.

It is also worth noting that this particular provider is banned on several underground discussion platforms because of sketchy billing operations. For instance, many users have complained about being billed for services, which they expected to be free.

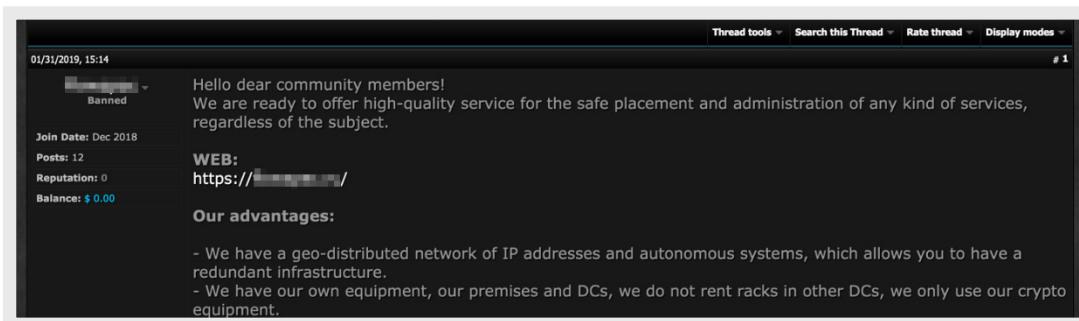


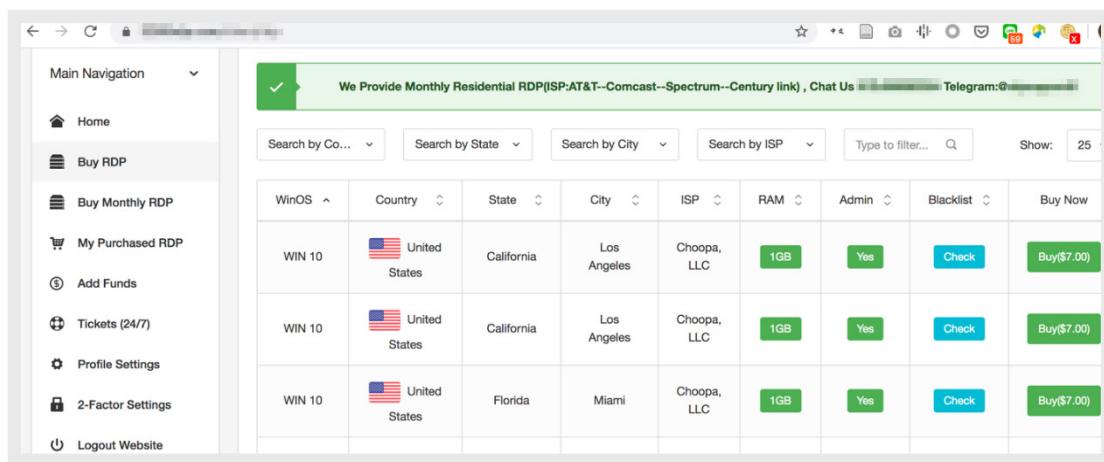
Figure 7. The same provider was banned in an underground forum

Compromised Legitimate Assets

Compromised Machines Used as Dedicated Servers

Compromised legitimate assets are often used for hosting during one or more steps of their criminal monetization lifecycle. Criminals use several methods to get access to the exposed servers. They can exploit vulnerabilities in server software, use brute-force attacks to compromise credentials, or initiate phishing and scam campaigns. Services targeted by these attacks may include SSH brute force, VNC brute force, and RDP brute force.³

Many successfully guessed credentials are then sold on online portals and shops, as seen below:



The screenshot shows a web interface for buying RDP services. On the left is a main navigation menu with options like Home, Buy RDP, Buy Monthly RDP, My Purchased RDP, Add Funds, Tickets (24/7), Profile Settings, 2-Factor Settings, and Logout Website. The main content area has a header "We Provide Monthly Residential RDP(ISP:AT&T--Comcast--Spectrum--Century link) , Chat Us" and a search/filter bar with dropdowns for Search by Co..., Search by State, Search by City, Search by ISP, and a "Type to filter..." input field with a "Show: 25" button. Below is a table listing three RDP service offers:

WinOS	Country	State	City	ISP	RAM	Admin	Blacklist	Buy Now
WIN 10	United States	California	Los Angeles	Choopa, LLC	1GB	Yes	Check	Buy(\$7.00)
WIN 10	United States	California	Los Angeles	Choopa, LLC	1GB	Yes	Check	Buy(\$7.00)
WIN 10	United States	Florida	Miami	Choopa, LLC	1GB	Yes	Check	Buy(\$7.00)

Figure 8. A screenshot of a site selling access to compromised RDP services

On the right side of figure 9, brute force, vulnerability exploitation, and other options lead to direct access to the server assets. However, many resources could also be acquired and accessed indirectly. On the left side of the same figure, several options can provide indirect access (they require extra steps from criminals). For example, this could be access to the infrastructure management software that allows for creating new instances of virtual machines or supply resources on a cloud provider. Meanwhile, access to accounts includes email accounts linked to these services in the cases where these emails can be used to recover passwords or already contain information that provides access to computational resources.

Attackers also often target websites that run popular content management system (CMS) software such as Joomla and WordPress, as many users run outdated versions of these software components, exposing those websites with older vulnerabilities. These vulnerabilities may not always lead to full server compromise but are often sufficient to allow attackers to place content on those websites. These “compromised” websites are often resold to be further used as landing phishing pages, exploit kit hosting pages, or SEO doorways.

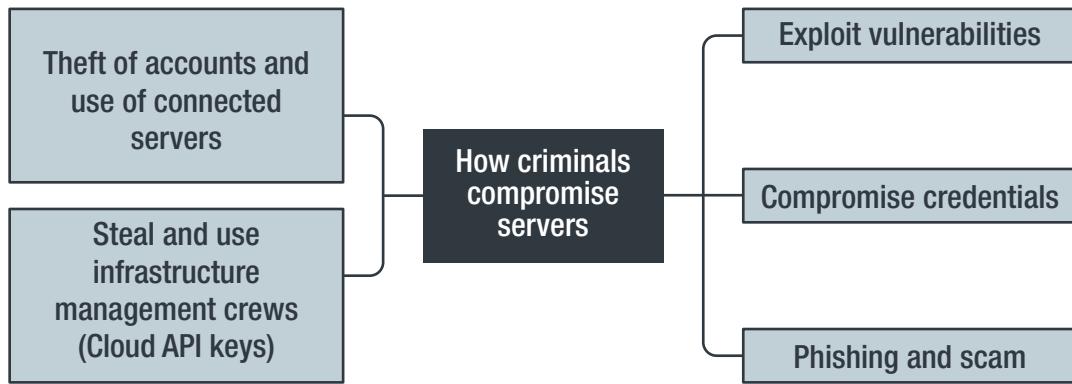


Figure 9. How criminals compromise servers

Many underground actors will initially target low-hanging fruits through brute-force attacks or well-known vulnerabilities. More sophisticated assets may require zero or one-day vulnerabilities, which has an open market for such. In the advertisement below, the author sells a vulnerability in the OpenSMTPD software, which allows users to compromise servers running FreeBSD, NetBSD, Debian, Fedora, and Alpine Linux, and use them for hosting purposes.

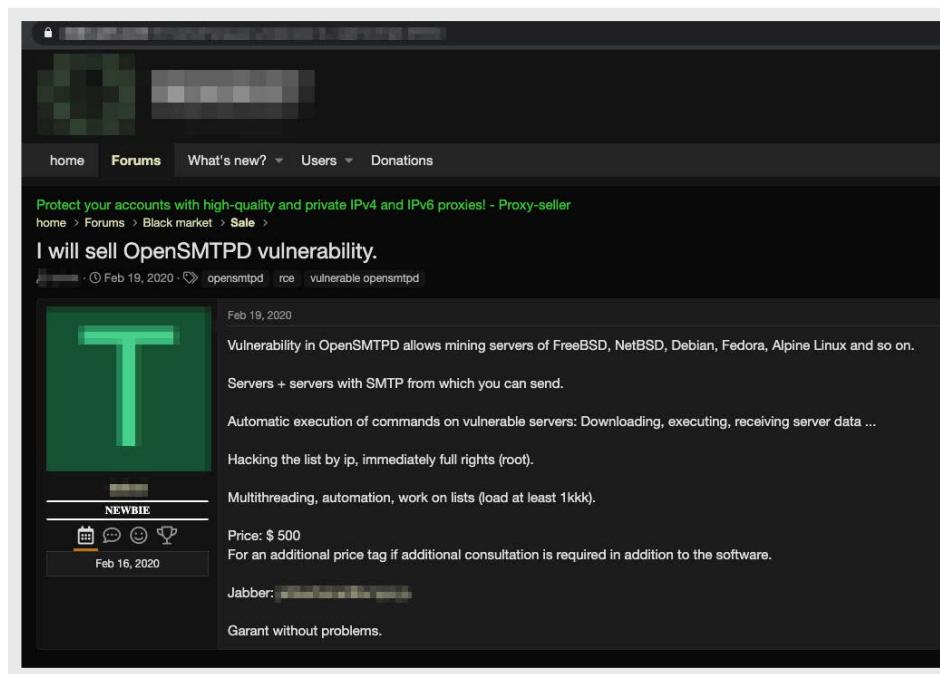


Figure 10. An advertisement of an exploit that allows actors to compromise and use exposed servers for hosting purposes

Once compromised, these assets will be sold in different places, ranging from underground forums and dedicated marketplaces to social networks (described in the first paper of this series).⁴

In the example below, compromised assets with login details are offered for sale in the Russian social media platform VK.

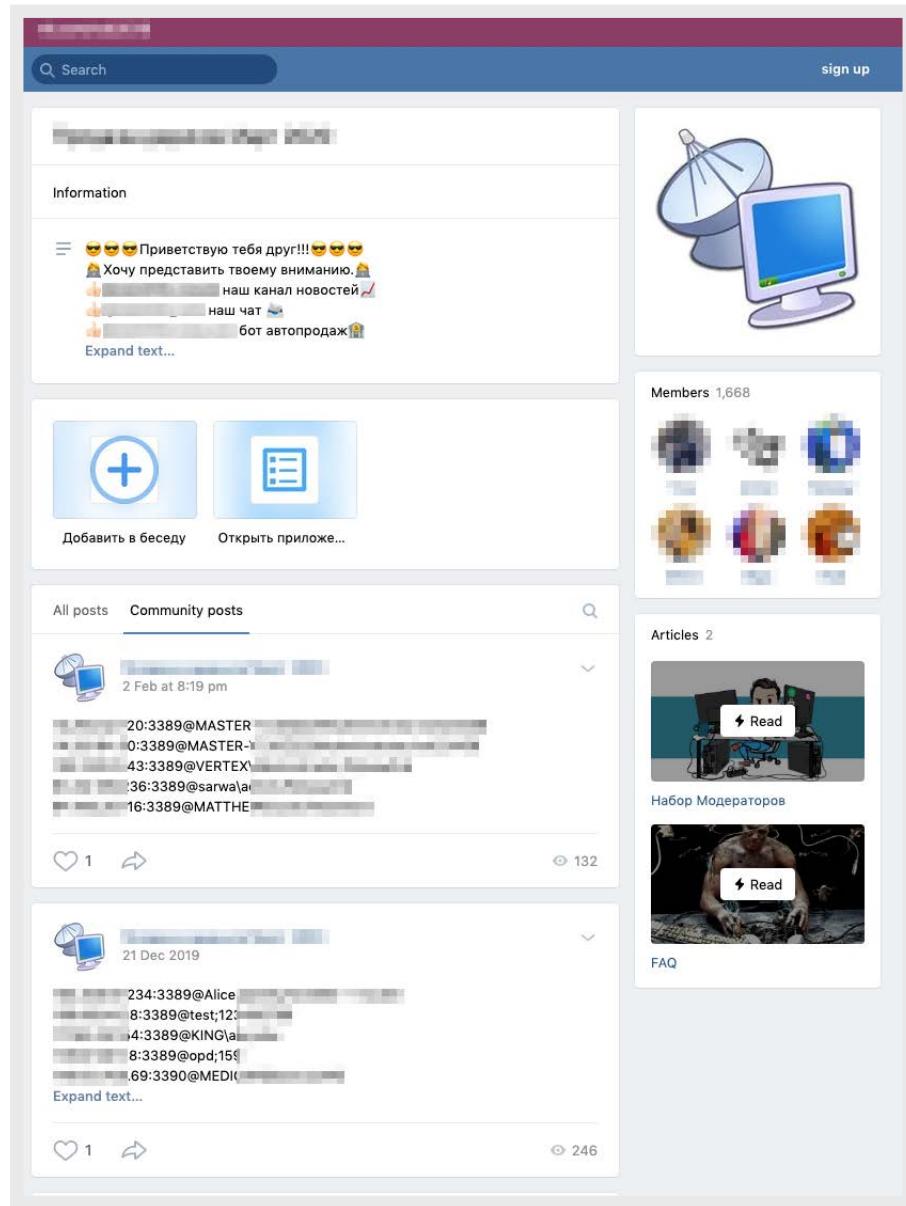


Figure 11. Credentials for compromised legitimate assets are advertised in a social media platform

A later comment in the thread suggests that almost all exposed assets were already affected by a CryptoLocker malware after one day after publication of this advertisement, showing the speed of movement of such assets in underground markets.

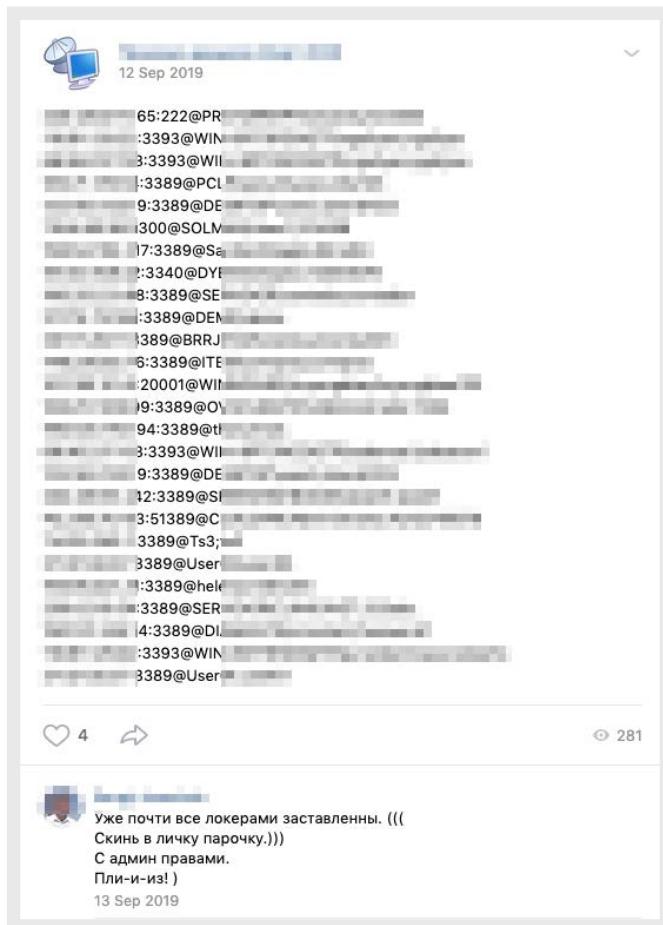


Figure 12. A posted claim that almost all assets in the post were already affected by CryptoLocker

Botnets for Rent (Regular PCs)

PC-based botnets have been around for many years. Even today, when we are witnessing a clear shift to mobile- and IoT-based botnets, PC-based botnets are still popular and have their particular niche. Underground actors have established mature ways of monetizing such botnets by reselling them or providing temporary access via a rental.

We have seen botnet rental services being used as a primary business model for particular attackers and in situations where available botnet resources exceed the level currently needed by their current controller. In other cases, we also saw botnet owners looking to rent botnets when they take a break from their business to update their tools that have been detected by a security vendor, expand their tools' features, or simply when the controller takes a vacation.

Figure 13 shows an advertisement for the rental of a PC-based botnet with over 1,000 connected PCs. The panel functions include DDoS, cryptocurrency-mining capabilities, and execution of arbitrary files. The list of permitted and prohibited activities is usually included in the advertisement; such services usually do not allow any files that have detections on VirusTotal, ransomware, or other crypto lockers, which would likely result in a machine that the botnet owner can no longer use.

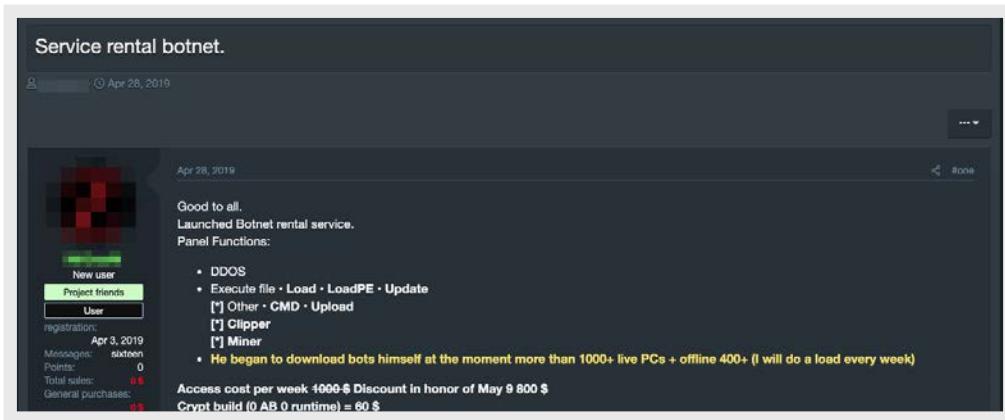


Figure 13. An offering of botnet rental service with access to the C&C panel

Prohibited activities will relate to both monetization schemes and control panel activities. The list of prohibited activities usually include the following:

- No ransomware monetization (because the compromise will be immediately exposed to the PC owner and the botnet controller will lose the bot)
- No removal of bots from the panel
- No panel setting changes
- No distribution of unencrypted binary files (encrypted binary provided by the controller) to avoid detection by security solutions

As a penalty for doing prohibited activities, the controller will often reject future access to the control panel.

Living off the Land: Abuse of Cloud and Hosting Services

Living off the land (LotL) tactics have been widely discussed in the context of hacker's toolkits.⁵ Such tactics involve the use of existing tools and infrastructure that threat actors repurpose for their needs, rather than building new custom tools or infrastructure.

The reason behind this is that threat actors have realized that their activities are harder to detect when they use off-the-shelf tools available on the machines in their kill chain. We observed that a similar tendency exists in underground hosting: The attackers are attempting to repurpose existing internet resources for their operations. This provides several benefits; there is an obvious cost-saving benefit to using free resources. The use of existing popular network resources also allows the communication to blend into an organization's existing network flows, making them more difficult for the defender to detect. In this section, we review some of the common cases of use and abuse that take advantage of such tactics.

Abuse of Cloud Hosting Services

Free hosting services exist to allow users to host some type of content without paying for it. These services are commonly tailored to novice users who need to host a domain name, an image, a blog, or a website. More advanced platforms, such as Microsoft Azure or Google App Engine, also allow the hosting of web application code. Other services provide free email or free online storage services.

Attackers also abuse such services, and we observed a variety of threat actors using them. One of the main reasons why these services are attractive to the attackers is because these make infrastructure disposable at little or no cost; in addition, free services provide a significant amount of anonymity by requiring very little information to register. The popularity of such services for legitimate purposes also makes their malicious use more difficult for an organization to detect.

In our research, we observed attackers using free services in the following scenarios:

- Free domains and DNS hosting are frequently used by attackers to procure disposable domain names for their infrastructure. We will discuss this in detail in the section focused on domain names.
- Free hosting services are often used to host malicious payload components. We have seen such services like Pastebin and GitHub used to host stages of obfuscated malicious payloads, which in turn are fetched by initial malware loaders. The use of these services allows an attacker to build disposable infrastructure, design multi-staged attacks, and push payloads to select targets that are of interest to the attacker. The attacker may also take the hosted payload down after the attack has taken place, making it harder for security researchers to analyze the attack.
- Cloud services provide advanced functions to users and are relatively simple to use. Attackers also figured out that they could proxy their C&C communication through cloud services like the Google App Engine to allow them to place more complex logic on these platforms.

Dropbox allows free account use if the user does not exceed its quota, as does Microsoft OneDrive and Google Drive. We observed that cybercriminals and targeted attack actors adapted techniques that use third-party cloud infrastructure as part of their C&C and data exfiltration platforms.

The example below shows a threat actor using a tool that supports multiple cloud storage options, allowing them to decide which platform to use at run-time.

```

0x00403ab8    50      push eax
0x00403ab9    8d4db4  lea ecx, [local_4ch]
0x00403abc    c745e44f6e65. mov dword [local_1ch], 0x44656e4f ; 'OneD'
0x00403ac3    c745e8726976. mov dword [local_18h], 0x65766972 ; 'rive'
0x00403aca    c645ec00  mov byte [local_14h], 0
0x00403ace    c745d0476f6f. mov dword [local_30h], 0x676f6f47 ; 'Goog'
0x00403ad5    c745d46c6544. mov dword [local_2ch], 0x7244656c ; 'leDr'
0x00403adc    c745d8697665. mov dword [local_28h], 0x657669 ; 'ive'
0x00403ae3    c745dc44726f. mov dword [local_24h], 0x706f7244 ; 'Drop'
0x00403aea    c745e0426f78. mov dword [local_20h], 0x786f42 ; 'Box'
0x00403af1    c645cc7c   mov byte [local_34h], 0x7c ; '1' ; 124
0x00403af5    e8d6e3ffff  call fcn.00401ed0 ;[1]
0x00403afa    8bf0      mov esi, eax
0x00403afc    c645cc7c   mov byte [local_34h], 0x7c ; '1' ; 124

```

Figure 14. A snippet sample from a tool that supports the use of Google Drive, Dropbox, and OneDrive for data exfiltration storage

In another example previously covered in a Trend Micro blog post,⁶ the Raccoon information stealer was seen using Google Drive as an intermediate C&C. The encrypted C&C information was stored in Google Drive as part of a filename. Interestingly, the attackers in this case hosted their main C&C infrastructure on the Google Cloud platform.⁷

From the perspective of network detection, this kind of network activity is much harder to detect because many organizations and security tools may simply whitelist IP ranges that belong to Google, Microsoft, and other large network companies.

From the perspective of the attacker, Google Cloud and Microsoft Azure are both very affordable resources because both allow “try for free” services with a registered credit card. This has led to an increased interest from attackers in collecting Google accounts with linked credit cards because those could be used to start instances of dedicated servers, as explained in the following tutorial.

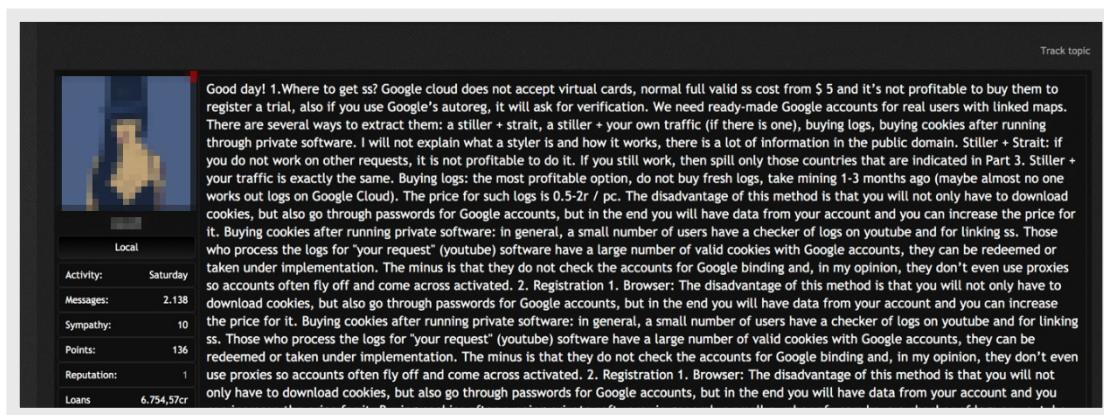


Figure 15. A tutorial on opening Google Cloud accounts from compromised Google accounts

There is also quite a lot of activity in buying and selling Google Cloud and Microsoft Azure accounts, like in the shop shown below, as well as in underground forums, social networks, and messaging platforms. The underground market related to cloud services is huge and is impossible to cover within the scope of a single research paper.

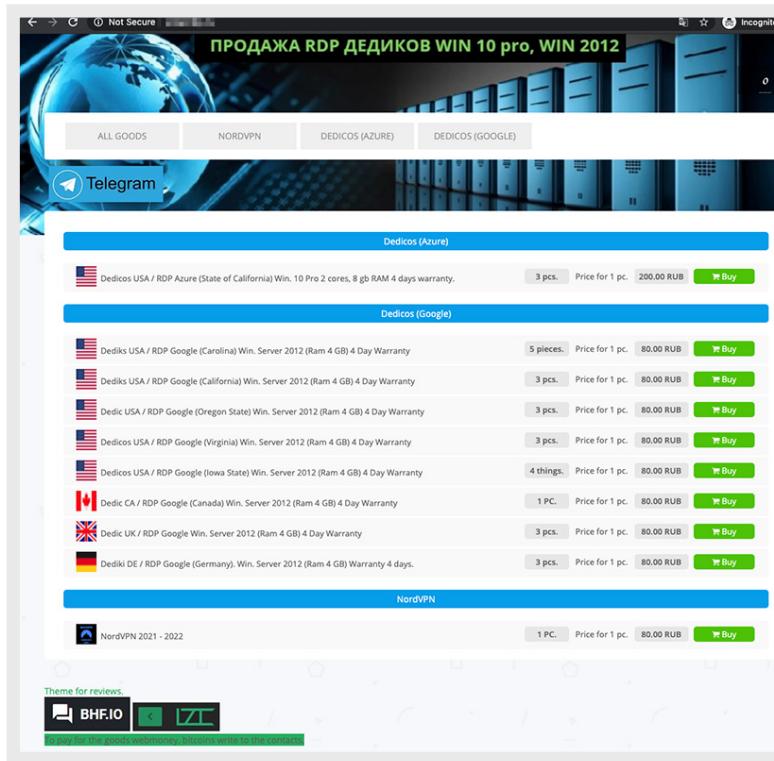


Figure 16. Microsoft Azure and Google Cloud accounts for sale

Abuse of Content-Hosting Services

As part of the living off the land strategy, attackers often use scripting languages like PowerShell and design multi-staged payloads. The scripted payloads make it harder for older signature-based antivirus (AV) tools to detect them. Having a multi-staged payload means that if the first-stage one is detected and mitigated, the second- and later-stage payloads would never be facilitated, thus the attacker would not reveal its C&C information or other components, giving a longer life to both C&C and malware modules.

The use and abuse of free content-hosting services are also very common in scripts. For example, in recent malware attack outbreaks, we observed many components that would attempt to fetch the content from a Pastebin-like location or a GitHub gist. In some cases, attackers place different bits of the script in different locations and then have the loader script reassemble the main payload.

Recent scans (2754 total)							<input type="checkbox"/> Show all
<input type="checkbox"/>	URL	Submitted	Size	<input type="checkbox"/> IPs	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	raw.githubusercontent.com/fossas/fossa-cli/master/install.ps1	6 hours ago	2 KB	1	1	1	
<input type="checkbox"/>	raw.githubusercontent.com/upinfoa/rch/up/master/dctar	8 hours ago	760 B	1	1	1	
<input type="checkbox"/>	raw.githubusercontent.com/upinfoa/rch/up/master/dctar	8 hours ago	762 B	1	1	1	
<input type="checkbox"/>	raw.githubusercontent.com/upinfoa/rch/up/master/dctar	8 hours ago	759 B	1	1	1	
<input type="checkbox"/>	raw.githubusercontent.com/upinfoa/rch/up/master/domtar	9 hours ago	759 B	1	1	1	

Figure 17. Code accessed from samples uploaded to urlscan[.]io from GitHub

We have seen other criminal groups actively using online hosting services to host their phishing pages.

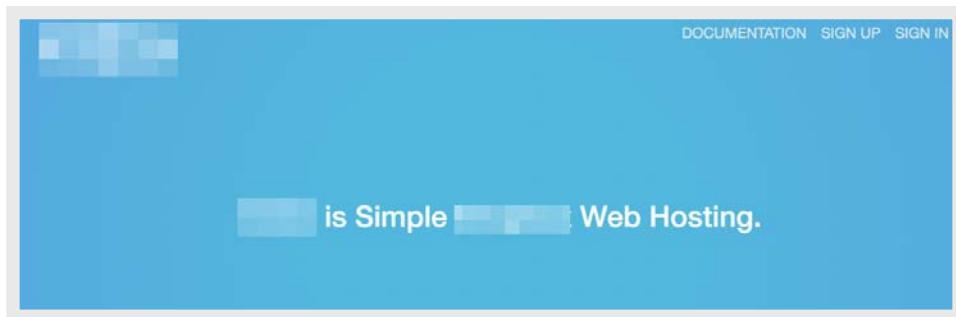


Figure 18: A service that hosts phishing pages

Criminal groups also use other free content-hosting platforms, such as online blogs and social media platforms. For example, a finance-oriented threat actor uses both YouTube and Blogspot to place information that encodes its C&C location.

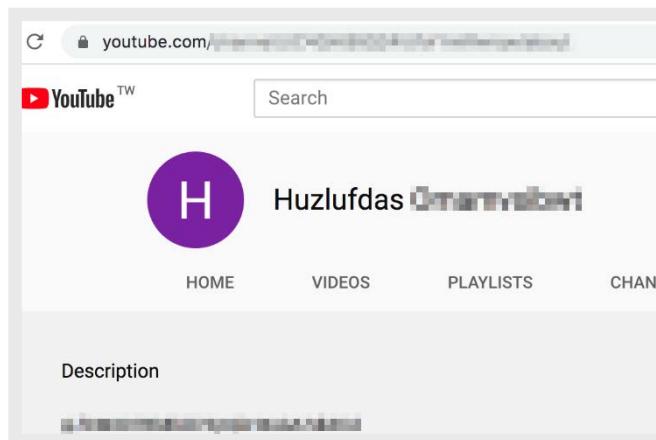


Figure 19. The description field holds encrypted content that reveals the C&C location

Privacy and Anonymizing Services

These services allow individuals to avoid disclosure of information that are considered sensitive. Many of the services outlined in this section are used by ordinary internet users every day. For individuals involved in illegal activities on the internet, however, privacy is a critical component of their operational security (OpSec).

The need for good OpSec is widely acknowledged by a variety of criminal groups, from terrorists to targeted exploitation groups and petty cybercriminals. After all, when a criminal's privacy safeguards fail, their true identity can be revealed to those investigating them.

Therefore, the tools and services that provide anonymity and privacy services are in high demand among a variety of criminal groups. Many of those online groups developed online tutorials to educate less-technically savvy group members about proper OpSec⁸ and invest considerable time in ensuring the reliability of this side of their infrastructure. The list below describes some of the most popular services.

Internet Overlay Privacy Networks

The Onion Router (**Tor**) is probably one of the most common tools for providing both privacy and anonymity. Indeed, we observed criminals frequently using Tor services to conceal their locations. However, some locations and organizations do consider the use of Tor networks as a red flag, and attempts have been made to proactively block it in some regions. Tor is not the only such internet overlay network, but while others such as Freenet, I2P, and other private community networks exist (e.g., Open Mesh, Guifi, and Freifunk), they are not as popular.

Steganography is a method used to hide information without standing out and attracting too much attention by way of concealing it “in plain sight.” Often, steganography-like communications are more suitable in hacker OpSec than the use of services like Tor.

Some of the tools used by criminals here are capable of establishing steganographic tunnels to prevent detection and blocking. A simple example of a steganographic network toolkit is a DNS tunnel software. It is frequently used to bypass filtered internet restrictions by “tunneling” all web traffic through DNS requests to a server under the control of the user. Attackers also often utilize steganographic techniques, both to conceal the network traffic patterns and the actual content. For example, we have seen images being used to embed both payloads⁹ and C&C information.¹⁰

SOCKS, Proxies, and SSH Tunnels

SOCKS and **proxy** services are probably some of the most common services. They allow threat actors to hide without attracting too much attention and triggering detections by network security monitoring tools.

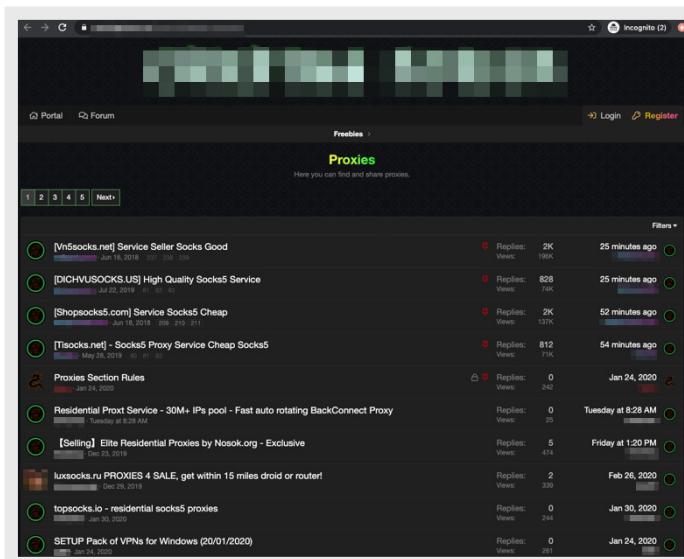


Figure 20. Proxy services for sale in a criminal forum

SOCKS is an internet protocol that exchanges network packets between client and server through a proxy server. SOCKS5 optionally provides authentication to authorized users. A SOCKS server proxies TCP connections to an arbitrary IP address and provides means for UDP packets to be forwarded.

SOCKS proxies are easy to buy in the underground. Many sellers accept cryptocurrencies. An example of an advertisement, including a price list from the seller that accepts Bitcoin and Ethereum cryptocurrencies is provided below.

Plan	Daily Limit	Price (\$)	Expired
Test	50	15	1 days
Daily 50	50	55	30 days
Daily 50	50	35	15 days
Daily 100	100	105	30 days
Daily 100	100	55	15 days
Daily 200	200	155	30 days
Daily 200	200	85	15 days
Daily 400	400	255	30 days
Daily 400	400	135	15 days
Daily 600	600	355	30 days
Daily 600	600	185	15 days
Daily 900	900	505	30 days
Daily 900	900	275	15 days
1 Year	50	505	365 days
1 Year	100	1005	365 days

Plan	Daily Limit	Price	Expired
Credit 50	Until Credit = 0	25	Unlimited
Credit 100	Until Credit = 0	55	Unlimited
Credit 240	Until Credit = 0	105	Unlimited
Credit 450	Until Credit = 0	205	Unlimited
Credit 900	Until Credit = 0	355	Unlimited

Here are the main advantages of using our proxy service:
Full proxy server support for protocols like SOCKS5Clear blacklist with whoer.net
Instant access after a payment has been made.
Option to choose a proxy server with IP-address of a particular country, region or even city.
Anonymity that we take very seriously, as our proxy servers do not keep any logs and never show your real IP-address.
Security that always open first, as all proxy servers run only within our partner program and are not public.
Methods of payment for Buy Proxy service
You will be directed to make a payment for the service immediately after registration of your personal account.
Currently, our proxy service automatically has been accepting electronic payments from Buy Socks Perfect Money, and WebMoney, BTC, DASH, ETH online payment systems.
For example, if you use WebMoney online payment system you need to follow these steps: go to a home > click Buy Socks> select icon WebMoney payment method direct . Payment of the WMZ through the system, and then click to continue to return to
For example, if you use BTC online payment system you need to follow these steps : go to a home>click buy socks>selection icon BTC payment method and flow the further instructions on BTC.
For example, if you use ETH online payment system you need to follow these steps : go to a home>click buy socks>selection icon ETH payment method and flow the further instructions on ETH.

Figure 21. An example of a price list for SOCKS proxies

Another means of concealing communication is wrapping it into a form of legitimate communication protocols. We can see that such tools as SSH tunnels are widely traded in the underground. Here is an example of a price list for SSH tunnels:

SSH tunnels SSH TUNNEL			
SSH Tunnels USA USA (Random Port) 100% Log In	2	0.91 \$	Buy
SSH Tunnels Canada Canada (Random Port) 100% Sign In	thirteen	1.10 \$	Buy
SSH Tunnels Switzerland Switzerland (Random Port) 100% Log In	2	\$ 1.68	Buy
SSH Tunnels Vietnam Vietnam (Random Port) 100% Log In	1023	0.65 \$	Buy
SSH Tunnels Belarus Belarus (Random Port) 100% Log In	0	0.80 \$	Buy
SSH Tunnels Germany Germany (Random Port) 100% Log In	0	1.52 \$	Buy
SSH Tunnels Australia Australia (Random Port) 100% Log In	6	1.52 \$	Buy
SSH Tunnels Brazil Brazil (Random Port) 100% Log In	9	0.57 \$	Buy
SSH Tunnels Belgium Belgium (Random Port) 100% Log In	0	1.17 \$	Buy
SSH Tunnels Argentina Argentina (Random Port) 100% Log In	9	0.66 \$	Buy

SSH Usa tunnels usa (america) By State			
SSH Tunnels Usa USA (America) State Georgia City Woodland 100% Log In Clean! Fresh!	38	\$ 1.35	Buy
SSH Tunnels Usa USA (America) Washington State City Redmond 100% Log In Clean! Fresh!	2	1.51 \$	Buy
SSH Tunnels Usa USA (America) State of California City of Los Angeles 100% Log In Clean! Fresh!	0	1.51 \$	Buy
SSH Tunnels Usa USA (America) State of Pennsylvania City of Barnesville 100% Log In Clean! Fresh!	3	\$ 1.65	Buy
SSH Tunnels Usa USA (America) New York State 100% Log In Clean! Fresh!	thirty	1.51 \$	Buy
SSH Tunnels Usa USA (America) Texas State 100% Log In Clean! Fresh!	0	\$ 1.62	Buy
SSH Tunnels Usa USA (America) Florida State 100% Log In Clean! Fresh!	8	1.51 \$	Buy
SSH Tunnels Usa USA (America) State MIX Random 100% Authorization Clean! Fresh!	104	1.18 \$	Buy

Figure 22. An example of a price list for SSH tunnels

An attentive reader may notice the price difference in SSH tunnels and different hosts, as well as the price difference between sold SSH access and, for example, RDP. The pricing of SSH tunnels is based on the country of location. The locations that are highly sought by threat actors are less available and more expensive (in accordance with free-market economy rules).

Location is very important for some illegal activities. For example, some credit card anti-fraud systems correlate the credit card owner information with geographical information of the IP address where the card use was attempted. Therefore, criminals are ready to pay more when they can buy a tunnel that matches not only the country but also the state and/or city.

Likewise, SSH services are generally more versatile than RDP and typically provide access to nodes that are less likely to go offline suddenly, thus its higher prices.

Anonymizing VPN Services

Underground actors often handle private pools of VPNs or proxies, which consist of compromised victim machines. They make use of these pools while conducting the additional malicious activities in which they specialize. Some of them have tried to monetize the idle time of such pools by providing VPN access for rent.

Some actors prefer to use commercially available VPN services, while others prefer to buy VPN services from an underground market or build their VPN hubs using software such as OpenVPN or SoftEther.

Other actors provide anonymizing services for rent as their primary business model. There are several signs that anonymizing service providers use underground infrastructures like compromised end-user or server systems.

One of the features that indirectly suggest a compromised or the gray nature of anonymizing services is an available “period of contract” or “period of warranty of availability” for the services. The shorter the numbers, the more suspicious these services are. It is barely possible to see an advertisement for a legitimate VPN provider, which says, “In case provided credentials doesn’t work during the next 24 (or 48 or 72) hours, new credentials will be provided for free.” But this is the normal case for underground sellers, as seen below.

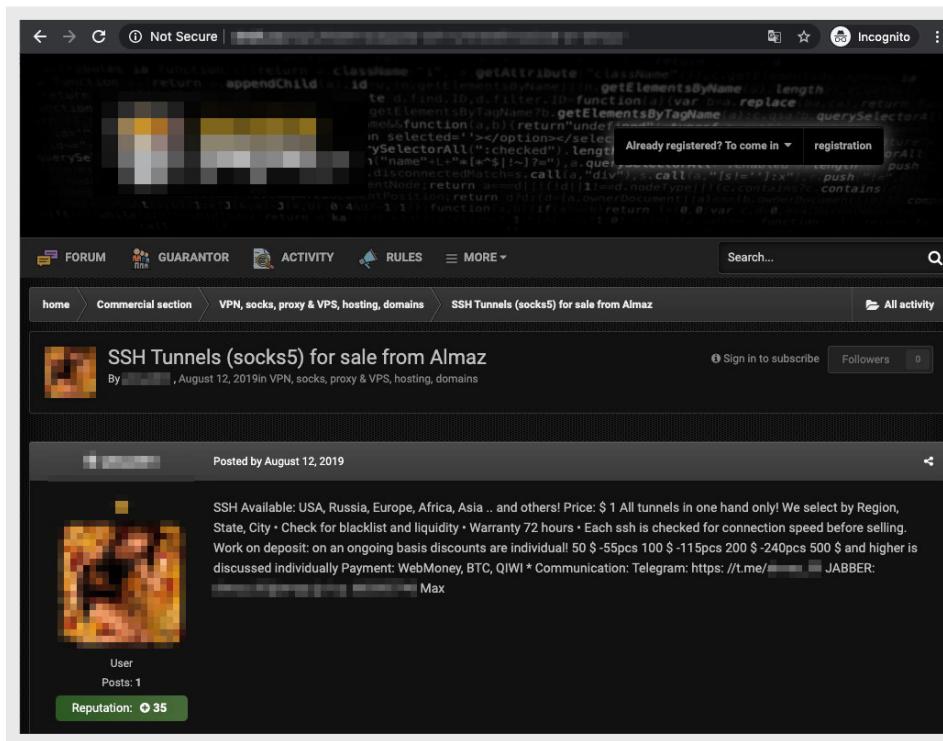


Figure 23. An advertisement of SSH tunnels with 72 hour-warranty sold in an underground forum

The second suspicious sign of the possible criminal nature of anonymizing services is the period of the contract. Many legitimate VPN providers consider monthly subscriptions as a minimum contract period. In criminal examples, however, we can see service offerings for periods as short as a single day. It is difficult to imagine legitimate use cases for a VPN that only require such a short period of activity. However, from a criminal perspective, there are plenty of situations, including phishing campaigns and carding. That's why VPN rental of very short-term subscriptions often look suspicious.

Below we can see an example of a provider that provides a one-day subscription option, advertises in the underground forums, and uses slang like “nosok,” which is a common term for “SOCKS Proxies” in the underground. The number of simultaneous connections mentioned in the advertisement allows subscribers to commit their malicious activities at scale. Many activities are carried out via VPNs and proxies, including:

- Validity check for lists of compromised credit cards or wallets
- Validity check for lists of compromised credentials (account stuffing)
- Account registration for cloud platforms and content hosting services
- Manipulation of content in social media platforms, coupon fraud¹¹
- Abuse of advertisement campaigns and other activities

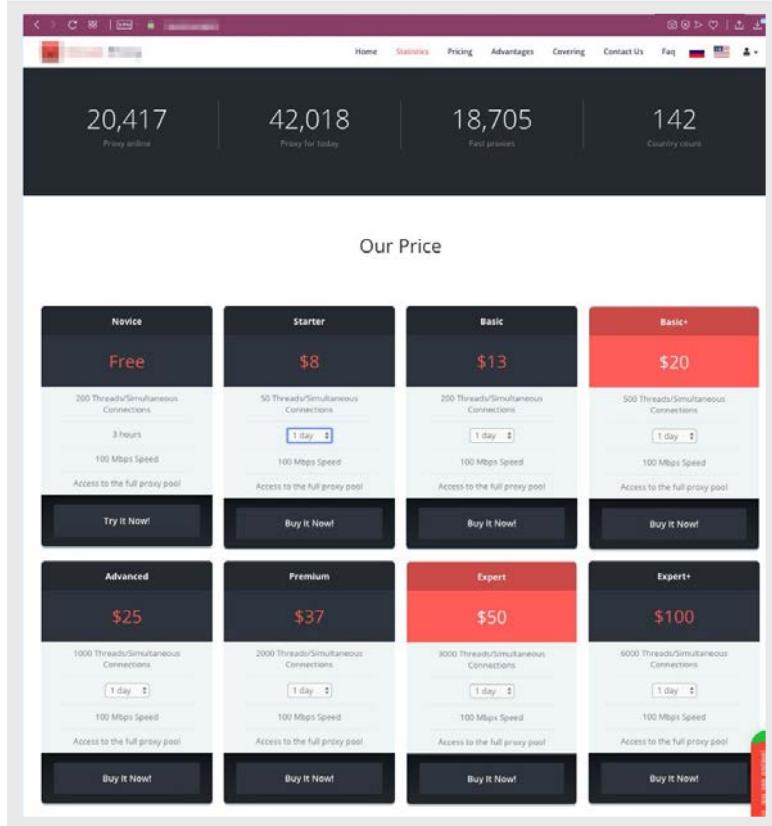


Figure 24. A VPN-selling site that advertises in the underground and sells short-term VPN contracts

Bypass Internet Restrictions Services

Internet restrictions and internet control have become very common in many countries. The underground marketplaces in countries with prolonged stringent internet control have developed a mature market for free and paid censorship bypassing services.

We observed that many of these services are popular among regular users and cybercriminals. We have seen some who use the services to hide their location, while others use it for criminal activities. Some VPN services declare themselves as “Privacy VPN, no logs kept” platforms and use this to deal with numerous abuse requests.

Many countries have information categories that are either permitted or prohibited on the internet. For example, gambling sites are not allowed in many religious countries in the Middle East. Authorities use legal procedures to regulate such content.

Abuse letters are often sent to hosting providers or the owner of the content. Some countries, such as China, the United Arab Emirates (UAE), Qatar, and Russia, have laws that enforce censorship. For example, in Russia, these centralized mechanisms allow blocking content using ISP equipment if the owner of the content or hosting declines to remove prohibited content three days after authority notification. We see some BPH providers explicitly saying that they will not host content that would be restricted in a country that is efficient at blocking on a nationwide scale.

Telegram is blocked in many countries as certain governments consider this messaging platform as harmful to their population, mainly due to its encrypted nature. Those countries' undergrounds have also developed a market for Telegram-enabling services.

As different countries restrict or monitor their citizens' internet use in different ways, different tools have also been built to help those citizens bypass these filters or monitoring. Naturally, any such system can also be used for criminal purposes looking to avoid detection, and they can even use the tools that were originally designed for a different region. Here are some tools we have seen used in this space:

Shadowsocks and ShadowsocksR

Shadowsocks (SS) is an open-source encryption protocol project from China. ShadowsocksR (SSR) is a fork of this project. Both of these protocols are widely used to bypass internet censorship in China.

The infrastructure that distributes information of available free SS and SSR services is well-developed and uses multiple channels, including web portals, messaging channels, and messaging bots.

Below is an example of a Telegram channel that pushes free updates of SSR lists daily:

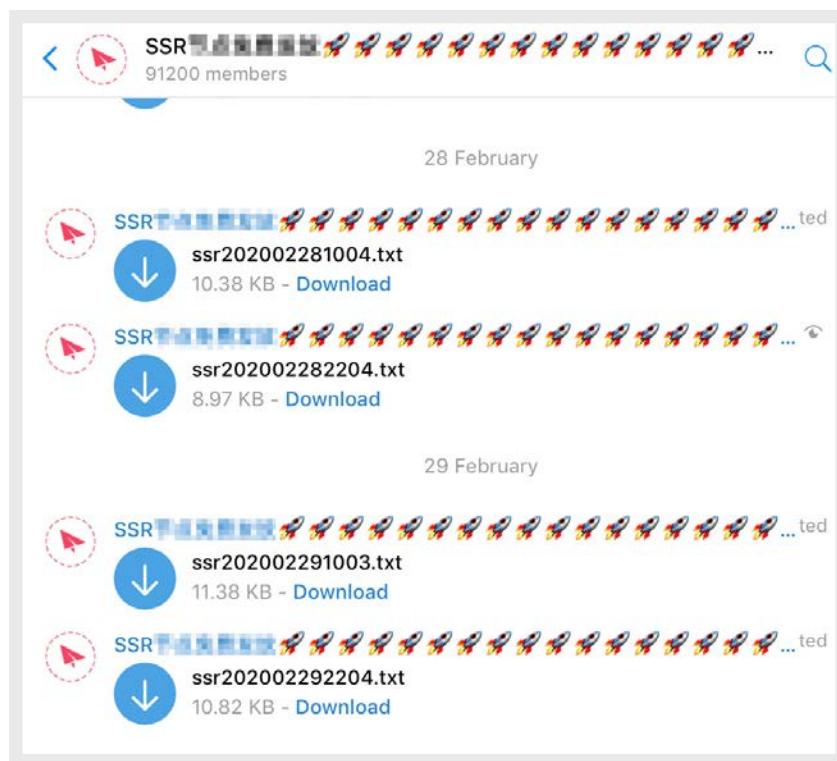


Figure 25. A Telegram channel that pushes free updates on SSR lists

Those who are unable to access those SSR services via Telegram (as they are also being blocked) can also obtain a list of SSR services via numerous websites:

IP	端口	密码	加密方式	协议	协议参数
xyz	543	http://t.me/xyz	aes-256-ctr	auth_aes128_md5	t.me/xyz
xyz	543	http://t.me/xyz	aes-256-ctr	auth_aes128_md5	t.me/xyz
66	21276	GWq6	aes-256-cfb	origin	
0.195	8097	eIWODni	aes-256-cfb	origin	
5.31	8099	eIWODni	aes-256-cfb	origin	
5.31	8097	eIWODni	aes-256-cfb	origin	
3.12	8097	eIWODni	aes-256-cfb	origin	
1.58	8099	eIWODni	aes-256-cfb	origin	
52	8099	eIWODni	aes-256-cfb	origin	
9.83	8099	eIWODni	aes-256-cfb	origin	

Figure 26. SSR services listing

As a result, these services are referred to as 紙飛機 (English translation: paper airplane) on many forums and web boards, which is a nod to the logo of Shadowsocks. The services that provide SS and SSR connectivity are then called airports (機場). This terminology eventually started being used on other similar services, so it has become common to see this category on proxying sites:

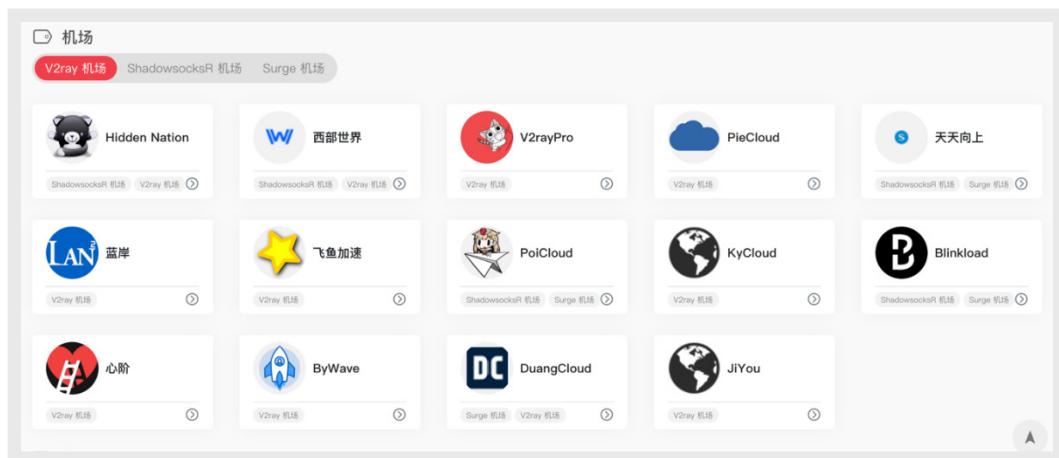


Figure 27. A screenshot from a proxying website showing “airports”

VMess/V2Ray

V2Ray is another protocol and platform that is popular in China and designed to proxy network traffic and bypass network restrictions. V2Ray consists of a set of tools that forms the core part of the Project V protocol, which is aimed at allowing anyone to build their private network over the internet. The network supports multiple protocols, including SS, custom routing, and obfuscation of traffic.

Numerous services exist to provide V2Ray proxying services. There are both free and paid services available. The paid-for services allow users to buy a service using a subscription-based model — buying a monthly, half-year, or one-year subscription — as shown in the following screenshot:



Figure 28. A screenshot of V2Ray proxy subscription portal

Payments could be easily done using one of the commonly available methods like scanning a QR code with Alipay:



Figure 29. Payment via QR code

Possession of this software could be considered a crime. Based on some underground forum feedback, the Deep Packet Inspection (DPI) engine of the Great Firewall (GFW) can detect plain SS/SSR and even some unrecognized encrypted traffic in some regions. This has caused users to seek the use of alternative methods that combine HTTPS with V2Ray or trojans that obfuscate traffic to make it look like communication to an HTTPS service. Combination chains of SS/SSR over TLS or V2Ray over TLS are also common.

There are multiple ways of chaining these protocols; a simple Google query reveals the most popular ones:



Figure 30. V2Ray autocomplete search hints

Other software that is also commonly used to bypass internet restrictions includes ChromeGo (bundle), Lantern (藍燈), Lightsocks, Trojan,¹² and ValdikSaS/GoodbyeDPI.¹³ Specialized projects such as Freegate and UltraSurf are also used.

Risks of Malicious Acceleration Services

Many of the proxying and acceleration services discussed are provided free of charge. Of course, some owners of these services seek to benefit from these, which should be clearly understood by the users.

For example, some of these service owners may monetize their service through some form of malicious behavior such as passive traffic inspection, traffic redirection, or traffic injection. An owner may attempt to generate additional clicks on their ads by running man-in-the-middle (MITM) attacks and injecting JavaScript ad tags into HTTP traffic, or stealing credentials.

Malicious acceleration services that require the use of closed-source software may also route traffic through the nodes running the software. The services are then sold in the underground.

It should be clearly understood that providers running proxy services such as SSR, V2Ray, and SOCKS do have their operational expenses. They also risk being arrested and prosecuted, as numerous cases have shown.^{14,15} So if the service is free, there must be a reason why the service is provided for free. It could be a lure by criminals themselves or a system that selectively intercepts or injects network traffic, or one that harvests user behavior information or credentials.

Domain Name Provision

Domain names are an important part of an attacker's infrastructure. An attacker needs to be able to use domain names that are harder to detect (i.e., one that can blend well with regular traffic) and provide a significant amount of anonymity and protection against a takedown.

Bulletproof domains have been part of bulletproof hosting operations for some time. For example, in the following screenshot, a popular bulletproof host offers abuse-resistant hosting for both IP addresses and domain names. As an extra option, he offers to notify the customers when any abuse complaints are received.

We also have seen offerings where a seller markets domains that have been recently freed or taken over and domains with an existing good reputation. Such domains are useful, as they can help bypass many reputation-based filters of security tools.

Such domains are also very useful when building doorways (for SEO) and other traffic landing pages, which are also used for spam and click-fraud.



Figure 31. A seller offering abuse-resistant hosting for both IP addresses and domain names

Some bulletproof hosts have a section in their offerings dedicated to bulletproof domain names.



Figure 32. A provider offers bulletproof domain registration

The use of free DNS services is also very popular; this topic will be covered in one of the subsections below.

Domains in Tor (And a Case Study)

The market for domains in the .onion zone is mostly related to illegal content. There are both offerings of onion sites' hosts and provision of components.

Some threat actors run online shops that simply sell domains with memorable or vanity names in the .onion zone. These domains can be generated given enough computing power from a tool like Shallot.¹⁶ The screenshot below shows popular domains on sale with prices in Russian Rubles. Domains in the top of the list cost about US\$80, while domains with eight signs cost around US\$10.

The screenshot shows a web interface for buying .onion domains. At the top, there are tabs for 'Main', 'Domain selection', 'buy onion domain', 'Creation of Tor site', and a British flag icon. A deposit of 0 is shown, along with a search bar and a 'Search' button. Below this is a header for 'ONION DOMAINS IN TOR | PRIVATE SOCKS 5 PROXY | VPN'. A note explains that unlike ordinary domain names, payment in the .onion zone does not require annual renewal; it's a one-time payment for full ownership. The main content is a table of domains categorized by length:

Product	N	For 1 pc.	
BEST SIGNS			
businessetc[REDACTED].onion	1	5130 ₽	
porneuevdu[REDACTED].onion	1	5130 ₽	
9 SIGNS			
porno3topic[REDACTED].onion	1	1250 ₽	
smartplexf[REDACTED].onion	1	1250 ₽	
sexe6cpixq[REDACTED].onion	1	1250 ₽	
wikileaks5[REDACTED].onion	1	1250 ₽	
8 SIGNS			
acoustically[REDACTED].onion	1	680 ₽	
activate7v[REDACTED].onion	1	680 ₽	
anarhisto[REDACTED].onion	1	680 ₽	
bestwarexy[REDACTED].onion	1	680 ₽	
blackbizn2[REDACTED].onion	1	680 ₽	
businessetc[REDACTED].onion	1	680 ₽	
casinov4c[REDACTED].onion	1	680 ₽	
creativeax[REDACTED].onion	1	680 ₽	
darkcoinfn[REDACTED].onion	1	680 ₽	

Figure 33. Price list for the domains in the .onion zone

Many bulletproof hosts are also willing to host onion sites. We conducted a short survey and identified real IP addresses of some of the sites hosted within the onion zone. It should be noted that this is not the case for all instances, and is usually only possible because attackers made fundamental mistakes in their setup. We did this by searching for .onion domain patterns within metadata of the systems, including banner names and SSL certificate fields, then comparing these to results gleaned from internet-wide scans on the regular internet.

For example, we found an underground market in an onion site related to a particular IP address hosted by a known cloud provider.

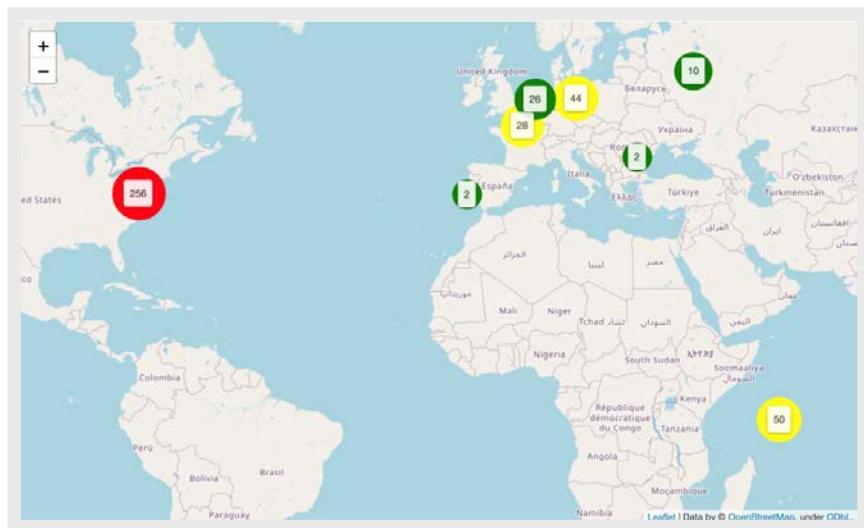


Figure 34. Map of ASN location for ASNs we found that hosted .onion sites

DNS Services Paid via Anonymous Payment Methods (Bitcoin)

Anonymous means of payment for domains are used not only by underground actors but could be used by activists, journalists, and whistleblowers. Such individuals might have very legitimate reasons to conceal their identity and protect their privacy and safety.

Therefore, there is a large number of hosting-related services that tailor offerings for this group of customers. These companies are not underground enterprises, but they are well-known managed DNS services that accept alternative means of payment. These are legitimate companies whose services happen to be also used by criminals in their respective activities. The services are attractive to cybercriminals since they accept bitcoin as payment.

The screenshot below shows a step-by-step guide on how to pay for managed DNS services in bitcoins.

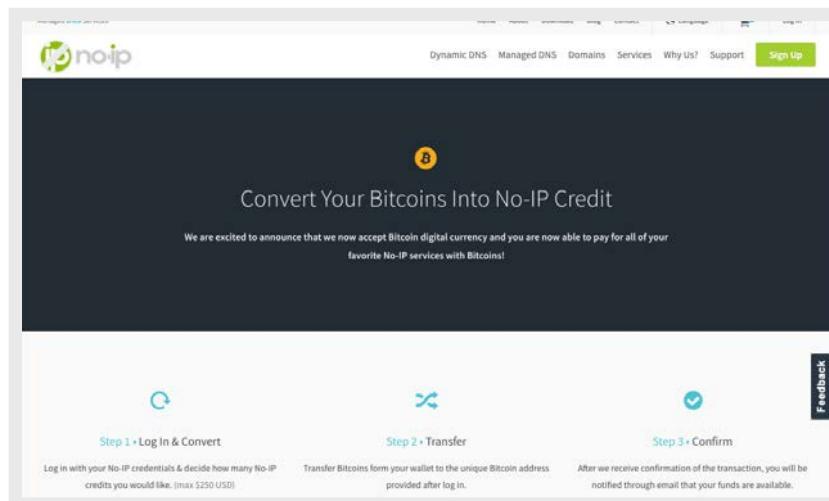


Figure 35. Bitcoin payments accepted by known DNS service

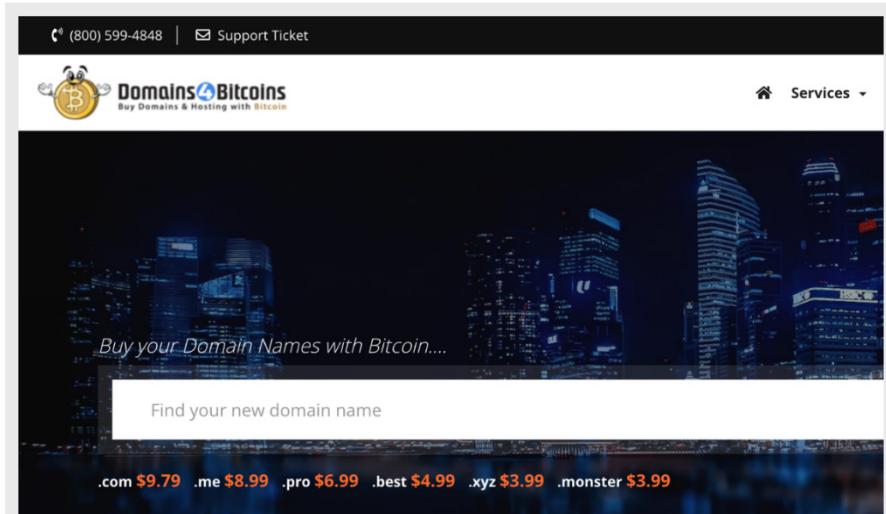


Figure 36. Another resource used by attackers to acquire and host their domain names

Even high-profile attacker groups like Lazarus used the aforementioned domain provision service in their activities.¹⁷ However, the use of this platform isn't limited to high-profile groups. It is sufficient to simply look into passive DNS records for some of the DNS name server platforms and see the scale of malicious use — from phishing to typosquatting — in the sample malicious domains purchased with bitcoin:

```
{BLOCKED}35exchanges329p29p7englehart.fun. IN NS 1a7ea920.{BLOCKED}n-dns.hosting.  
{BLOCKED}35exchanges329p29p7englehartsafemail-tuduma.fun. IN NS 1a7ea920.{BLOCKED}  
n-dns.hosting  
{BLOCKED}newport.ooo. IN NS 1a7ea920.{BLOCKED}n-dns.hosting.  
{BLOCKED}s-es-05798.ooo. IN NS 1a7ea920.{BLOCKED}n-dns.hosting.  
{BLOCKED}s-es-15324.ooo. IN NS 1a7ea920.{BLOCKED}n-dns.hosting.  
{BLOCKED}s-es-70263.ooo. IN NS 1a7ea920.{BLOCKED}n-dns.hosting.  
{BLOCKED}s-es-89071.ooo. IN NS 1a7ea920.{BLOCKED}n-dns.hosting.  
{BLOCKED}lectronica-abanca.ooo. IN NS 1a7ea920.{BLOCKED}n-dns.hosting  
{BLOCKED}rum.org. IN NS 1a7ea920.{BLOCKED}n-dns.hosting.  
{BLOCKED}rum.org. IN NS 1a7ea920.{BLOCKED}n-dns.hosting.  
{BLOCKED}umn.top. IN NS 1a7ea920.{BLOCKED}n-dns.hosting.  
{BLOCKED}unm.top. IN NS 1a7ea920.{BLOCKED}n-dns.hosting.  
{BLOCKED}uum.top. IN NS 1a7ea920.{BLOCKED}n-dns.hosting.  
{BLOCKED}erwalletr.top. IN NS 1a7ea920.{BLOCKED}n-dns.hosting.  
{BLOCKED}ermalletr.top. IN NS 1a7ea920.{BLOCKED}n-dns.hosting.  
{BLOCKED}erwallett.top. IN NS 1a7ea920.{BLOCKED}n-dns.hosting.  
{BLOCKED}erwalletr.top. IN NS 1a7ea920.{BLOCKED}n-dns.hosting.  
{BLOCKED}erwallets.top. IN NS 1a7ea920.{BLOCKED}n-dns.hosting.
```

Certificates for Domains

Cryptographic certificates are an important part of an attacker's domain-related toolchain. Such certificates could be used on SSL-enabled HTTP(s) servers to host components of an attack and attempt to stay invisible to some network monitoring tools through running traffic via HTTPs. Free-signed SSL certificates are quite sufficient in this case.

Other attackers orchestrate phishing attacks or MITM traffic interception, and they need certificates that match the hostname or domain name of a target organization. We looked into several targeted attacks in the past where an attacker specifically applied for a certificate using “*.VICTIMDomain[.]ccom.” The attacker likely invested in this asset to design realistic-looking phishing landing pages and more.¹⁸

Various threat groups commonly use free SSL certificate services; we have often seen them use certificates issued by letsencrypt[.]org and Comodo.

Decentralized DNS

Recently, blockchain and decentralized DNS top-level domains (TLDs) have become an innovation for threat actors, even though we wrote about their potential for misuse as early as 2013.¹⁹

The most prominent players in this space are Bitmessage, Emercoin TLDs, and Namecoin (.bit domains). The associated TLDs we have seen are .bazar, .bit , .coin, .emc, .eth, and .lib namecoin.

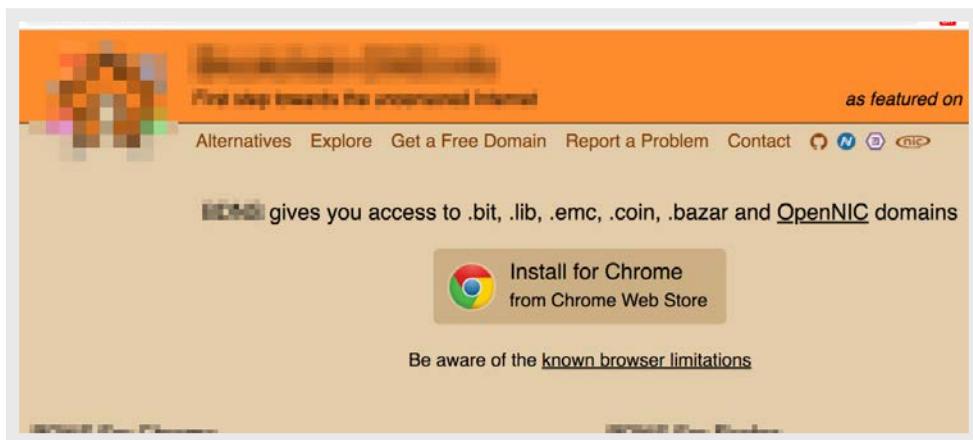


Figure 37. A site that allows registering Namecoin and Emercoin domains

Namecoin service data is stored in its blockchain, while names and values are attached to coins with a value of 1 NMC. Registration of these domain names could be done through the tools provided by Namecoin or using third-party registrars.

Users get charged after each transaction. They can become the owner of the domain name after the first two transactions (name_new and name_firstupdate).

The TLD's distributed architecture, resistance to a takedown, full anonymity, and ability to fully automate domain name operations, make this TLD very attractive to attackers. One of the prominent domain names hosted within this space was gandcrab[.]bit, which was associated with the infamous GandCrab ransomware (other domains used by the same malware strain are carder[.]bit, ransomware[.]bit, and zonealarm[.]bit).^{20, 21}

Emercoin TLDs are peered top-level domains. These TLDs are accessible from the OpenNIC network but are not managed by them. GandCrab is an innovative adaptor of this technology, and one of the domain names that it has been using is nomoreransom[.]coin. The domain name is a deliberate pun on the legitimate No More Ransom project from Europol and other partners (including Trend Micro), which provides decryption support for several ransomware families.

Bitmessage is an alternative to DNS communications that also uses blockchain for communication. We foresee malware herders adapting this P2P protocol in the future.

Dynamic DNS Services

Attackers commonly use dynamic DNS services for their C&C infrastructure. We have seen both cybercrime and targeted attack groups using various dynamic DNS providers. The main reason for this is that dynamic DNS allows short TTLs so that attackers can quickly switch between IP addresses or to only point the domains to the real C&C server when the C&C server is in use, which minimizes the chances of discovery.

We believe another reason why dynamic DNS services are frequently used is that their TLDs are often classified as benign and whitelisted, and defenders need to track and document the second-level domains carefully.

We have seen different threat actors using these providers, including the ChessMaster's RedLeaves toolkit²² and the Adwind cross-platform RAT.²³

Free DNS Hosting Services

Free DNS services have long been a favorite source of domain names for criminals. There are several reasons behind this. Most of the free DNS services perform little to no validation of the person registering a domain name. Free DNS services are also popular for legitimate use, so there is quite a large amount of traffic to blend in with. While free DNS services may not provide a sufficient amount of protection against takedown, the low cost (or no cost) of domain name acquisition is a big attraction.

Another issue that we identified with some free DNS hosting services is a feature that allows for the creation of a subdomain of existing domains within the free DNS hosting service. This is attractive to attackers that look to subvert reputation-based detection mechanisms.

Several free DNS hosting services are frequently used and abused by attackers. We have seen free DNS services being used for both C&C and exploit kit-serving infrastructure. For example, threat actors frequently use the free DNS host afraid[.]org this way. The host allows free and paid-for DNS hosting. One of the features of free DNS hosting on the site is that anyone could create subdomains of domain names hosted on it.

We encountered legitimate domain names being abused in this way. Adwind²⁴ malware has also made use of this approach.

Emerging Trends in Underground Infrastructure Services

In this section, we will describe some of the emerging trends that we observed in underground hosting. The services listed here are not as common as those that have been detailed earlier; these either cater to very niche clients or represent new, emerging trends that we expect to become more popular over time.

Mobile Workspace

During our research, we came across an interesting service offering. Figure 38 shows a snapshot of this vendor's website:

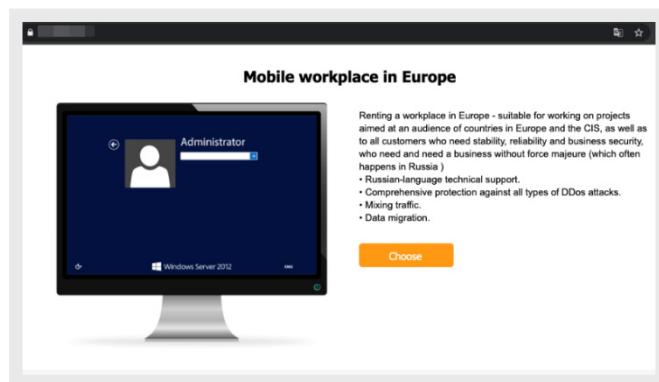


Figure 38. A mobile working environment service in Europe

This vendor specializes in providing mobile-working environments, including “Mobile working environment in Europe” and “Mobile working environment to work with graphics.” Each mobile-working environment comes with preinstalled specialized software, which the user may require for work (i.e., the graphic environment is preinstalled with graphic and video editing software.)

What makes this provider interesting from a cybercriminal perspective is that it offers “Mobile working environment: Bastion.” This is a bulletproof variant of a working environment. The provider guarantees that no third-party would be able to gain access to this environment and provides several features that are attractive to cybercriminals.

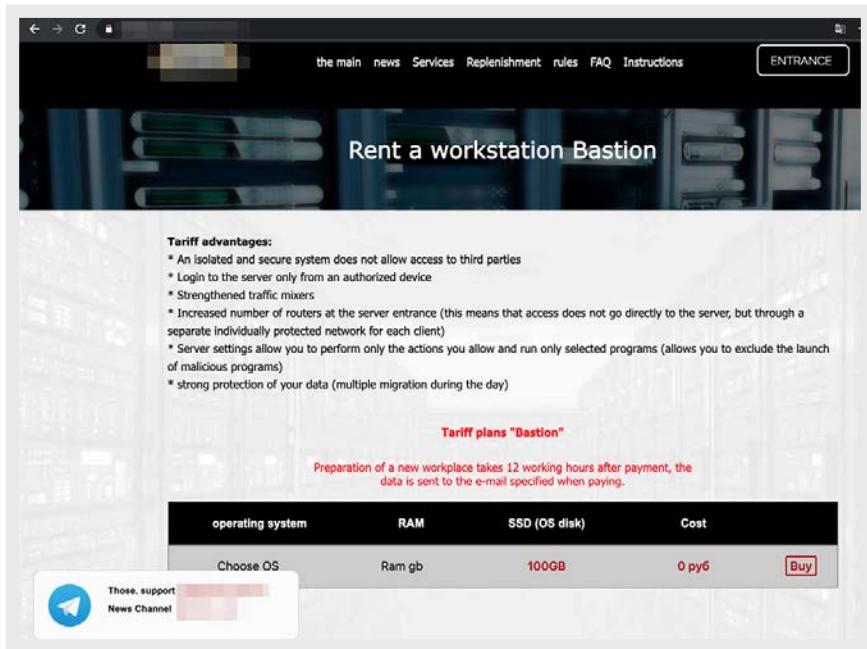


Figure 39. Mobile-working environment Bastion

Although the website owner's policy forbids the distribution of malicious software, we found a detailed advertisement on a forum hinting that other malicious activity is acceptable:

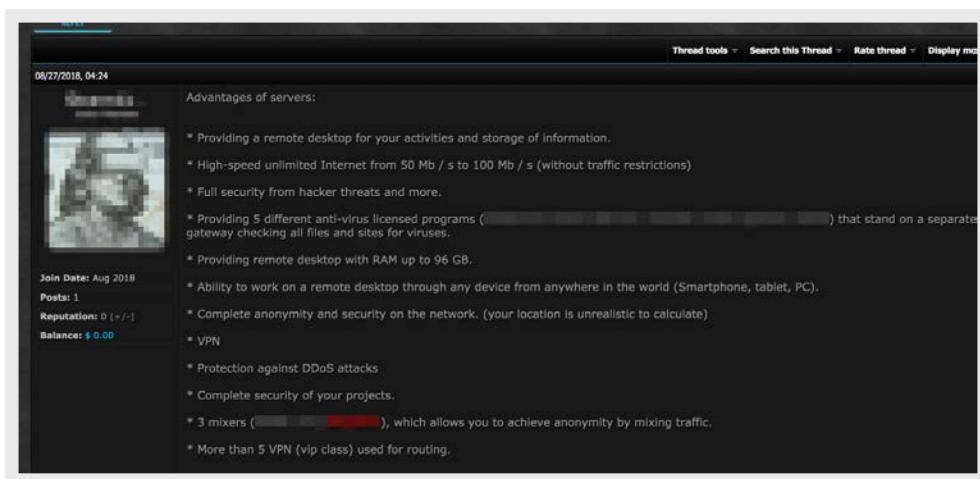


Figure 40. An advertisement of a mobile-working environment in an underground forum

Among other features, the offer mentions complete anonymity, to make it impossible to identify the user's location; high-speed internet connectivity; DDoS protection; an outgoing traffic mixer; and five different VPNs. While direct port-scanning, brute-force, and malware distribution are not allowed, the attacker can conduct other criminal activities from these systems.

This is not the only instance of such a service. We also identified a similar service advertised on another criminal forum — this time a bulletproof workspace hosted on the Tor network:

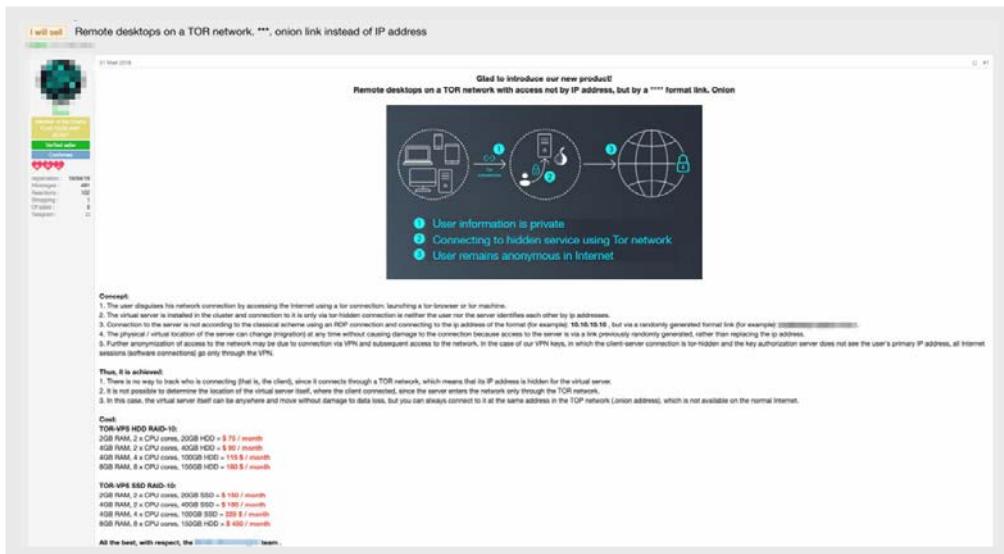


Figure 41. Threat actor offering a bulletproof preconfigured workspace on Tor

This same seller offers a variety of other products and services, including a fast-flux service, customized routers, VPN services, a SIP+SIM package, and their own “secure” Android variant.

Interestingly, this vendor also offers a service that physically removes certain components from devices such as a mobile phone or a router then mails the device and these components separately back to the customer.

For example, if the cybercriminal is concerned that law enforcement might tamper with their devices’ audio recording, the criminal only uses this phone for SMS messaging, and they could physically remove the microphone and camera from the phone.

If they are concerned that the device could be compromised through a vulnerable Bluetooth chipset, that also could be removed.

This service costs €50; the vendor even provides a video demonstration on YouTube:

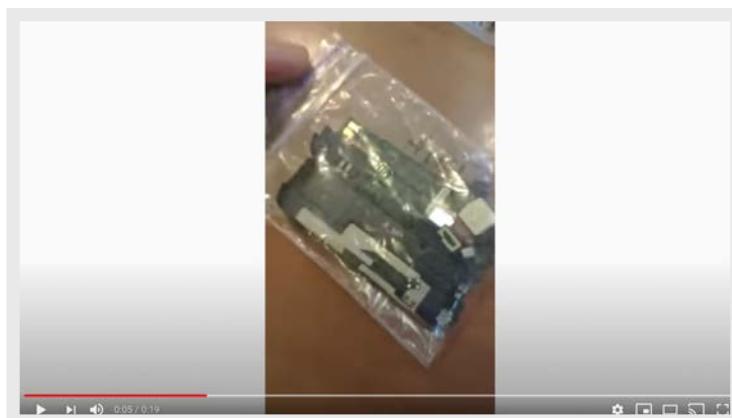


Figure 42. Components removed from the device before shipping to the user

Traffic Mixing Anonymizing Networks

Criminals use numerous services — this report has already mentioned Tor and other similar services — to anonymize traffic on systems.

We have seen other similar, known proxy network services mentioned on forums. The earlier mentioned mobile-working environment service has also developed an in-house encrypted traffic mixer using geographically distributed routers.

Some even combine this traffic mixing with anonymous VPS machines that periodically move from data center to data center, often located in different geographical and juridical locations, making the tracing of such systems even more difficult.

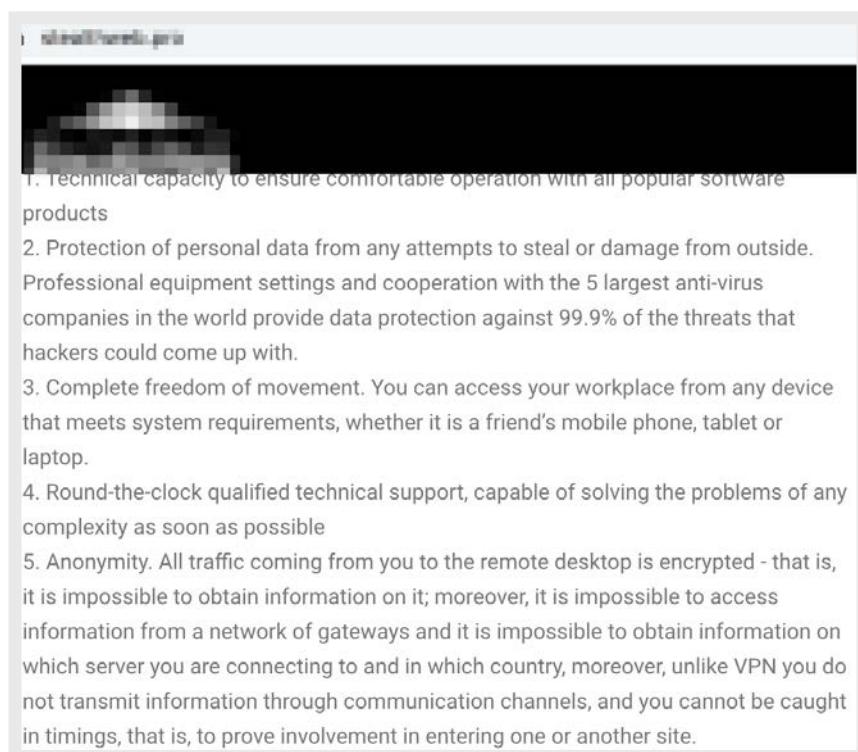


Figure 43. An anonymous VPS service

Custom services are also available for combining VPN connections, Tor connections, JAP, and geographically distributed sets of routers. These combinations form a complex chain of encrypted machines and traffic redirection that would be exceptionally difficult for an investigator to trace. One service offers the following redirection chain:

- Encrypted machine – VPN1 – VPN2 – TOR - Single gateway for bouncing traffic -Traffic mixing service
 - Traffic bouncing through geographically distributed routers -Remote desktop (for operations)
 - Connecting through other geographically distributed routers – Tor servers – Exit node – Final destination



Figure 44. Traffic obfuscation chain of a service describing the complex network routing it offers

Parasitic Computing for Rent

Attackers have been very creative with creating value from the resources that they have compromised. One of the important developments that we observed in the underground market is the supply of parasitic computing resources.

We observed several variants of this service that attackers have created.

HVNC and HRDP

HVNC, also known as Hidden VNC, is a feature that has been a part of some malware strains from 2014 to 2015. The HVNC component creates a hidden desktop on a compromised machine and allows the botnet operator to run software applications in parallel with normal system use by the machine's owner. The output of these applications is displayed on a hidden screen and will not be visible to the victim.

A screenshot of a forum post. The post is by a user named 'peron_shells' (Observer). The post content includes:

[SHOWTOGROUPS = 3,4,51,23]
Good day!
He resumed work and is pleased to present his product to you:

BMW hvNC

Functionality:
hvNC runs on win7-win10 lines
Excellent desktop rendering
chrome
IE
ff
Loader

Rental price (10 seats for rent):
\$ 1500 a month
hvNC + Loader
Included in the price is a full support service
online 16 hours a day, 6 days a week

License purchase
4,500 \$
200 \$ rebuild
Updates for a fee

Figure 45. A sample of HVNC for rent

This example supports Windows 7 and 10 platforms and allows operators to run the browsers listed in an HVNC environment. The toolkit comes with a control panel that allows browser injections and execution of binary files on compromised machines.

The HVNC offerings have developed into a solid market of its own with several attackers focusing on building and marketing these virtualized parasitic platforms. HVNC has become so popular that we have seen requests for HVNC development on online freelancing platforms.

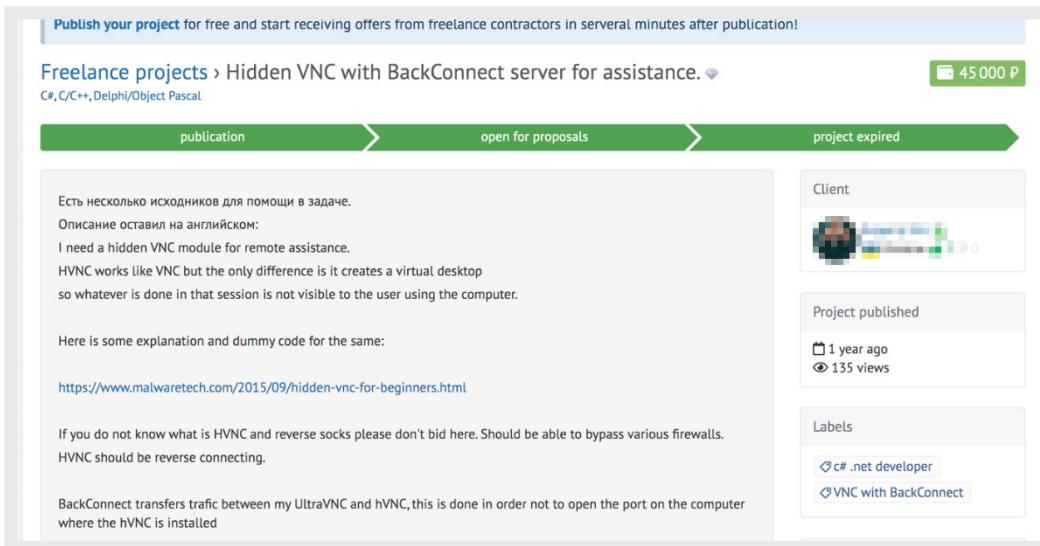


Figure 46. An RFP request for HVNC connectivity with Backconnect server

Later evolutions of this approach led to the development of HVNC variants that supported the more user-friendly RDP protocol called HRDP in underground discussions.

Mobile Infrastructure

Proxies hosted on a mobile infrastructure are now playing an important role in several segments of the underground ecosystem. They are often used by actors that commit activities at scale and impersonate legitimate potential customers. These include traffic arbitrage, a business model in which you buy traffic at a lower cost and redistribute it to monetize it; social media marketing (SMM), the use of social media platforms and websites to promote a product or service; registering accounts in social networks; coupon fraud; and promotional campaigns for social media manipulations. This is partly due to a higher level of trust being given to mobile traffic versus desktop traffic by some sites. In these cases, Android emulators are often used together with proxies.

There are two main types of mobile proxies: ones based on an actor's infrastructure and ones based on compromised mobile assets.

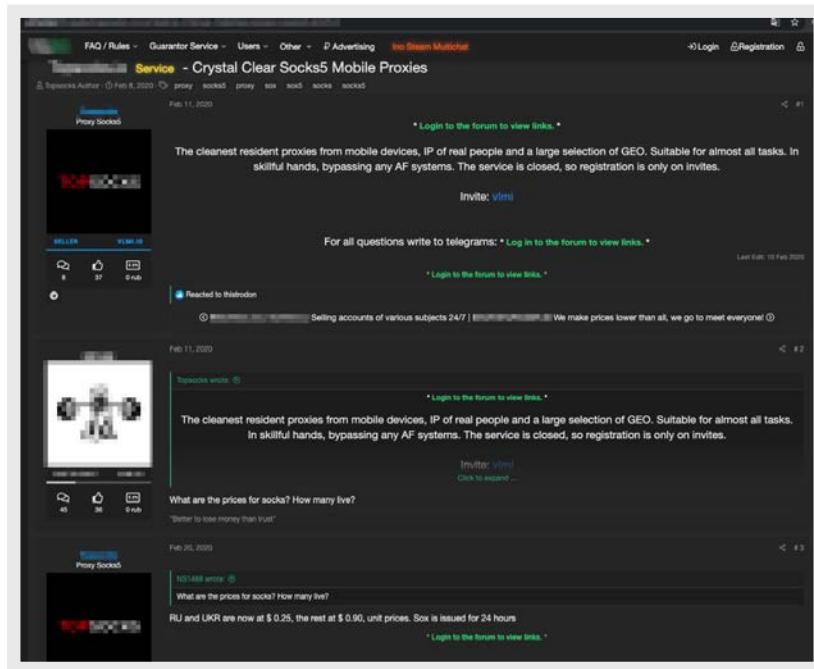


Figure 47. An advertisement for mobile proxies based on victimized mobile devices in different geographical locations

One of the important features for attackers' mobile proxies is that they use IP pools of mobile phone operators, which have limited size relative to the number of devices connected through these pools. As a result, the providers must rely on some level of network address translation (NAT) infrastructure, whereby multiple users share an external IP at a given time. In turn, this setup limits the ability to blacklist such pools because blocking will often affect large numbers of legitimate customers.

Some criminal service providers even organize customer polls about the most important geo-locations for the proxies to inform their future strategic decisions.

Poll [REDACTED]

Need some special GEO proxy? Choose from the list, and we will try to implement!

* Required

Which mobile proxies would you like to see on [REDACTED]?

- India
- Spain
- Poland
- Sweden
- Ireland
- Regions of the Russian Federation
- Other: _____

Mail your [REDACTED] account

Leave your mail to which your [REDACTED] account is registered to receive a 5% discount on a proxy order

Your answer

Figure 48. A poll on preferable geo-locations for mobile proxies

IoT Hosting Infrastructure

Underground actors widely use compromised and purchased IoT equipment to host services. Compromised assets are mostly weaponized to commit DDoS attacks and provide anonymization services. We also witnessed other rarely occurring cases that involve the use of routers²⁵ or video-processing IoT equipment for cryptocurrency mining. As such cases have been covered in-depth in a previous Trend Micro research paper,²⁶ this section will only highlight two examples.

We found customized IoT equipment sold in underground forums as hardware-based anonymization tools. In the advertisement of “Secure 4G VPN router” below, we can see a note in the bottom that this actor offers customized solutions based on routers from MikroTik, Linksys, and other hardware vendors, requiring knowledge of multiple hardware, firmware, and software of IoT equipment.

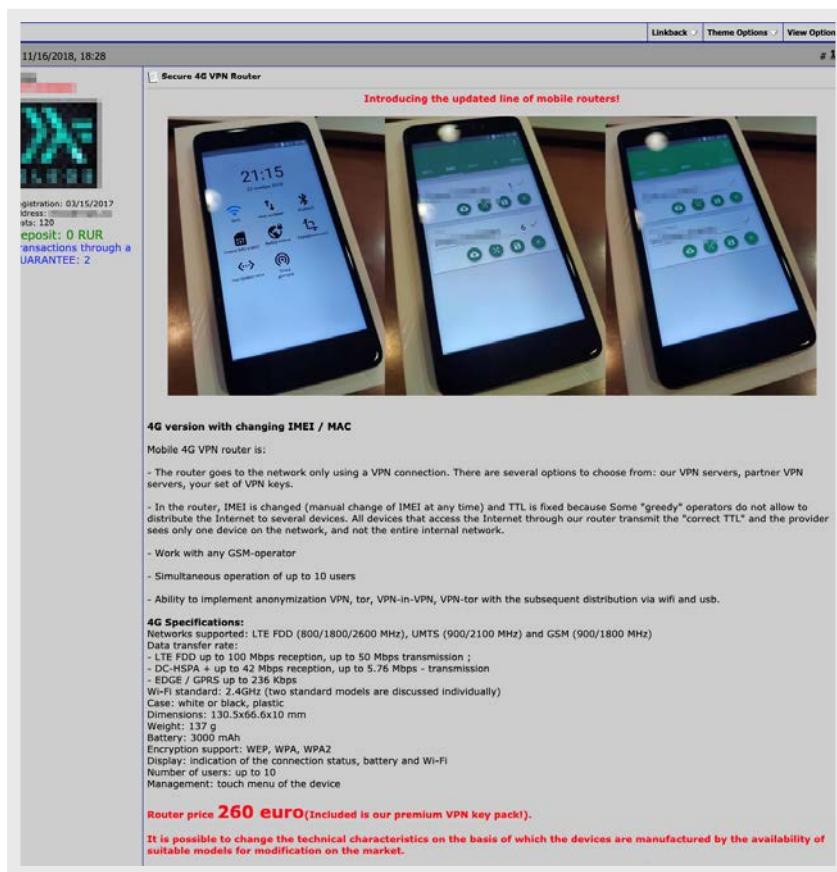


Figure 49. An advertisement of stationary hardware solutions for VPNs

The second case of compromised routers with preinstalled VPN configurations is interesting because of the price — they were being sold in the underground for US\$13. This is high for such an offering, and the actor highlights the potential use of these routers for PayPal and banking fraud. For these kinds of activities, especially for credit card fraud, actors try to find internet access points that are as close as possible to the credit card billing address. These transactions will be less suspicious for the banks' anti-fraud systems, and in some cases, will not trigger second-factor authentication requests. The high price likely indicates that these compromised routers can be precisely categorized up to the postal index or city name by the seller.

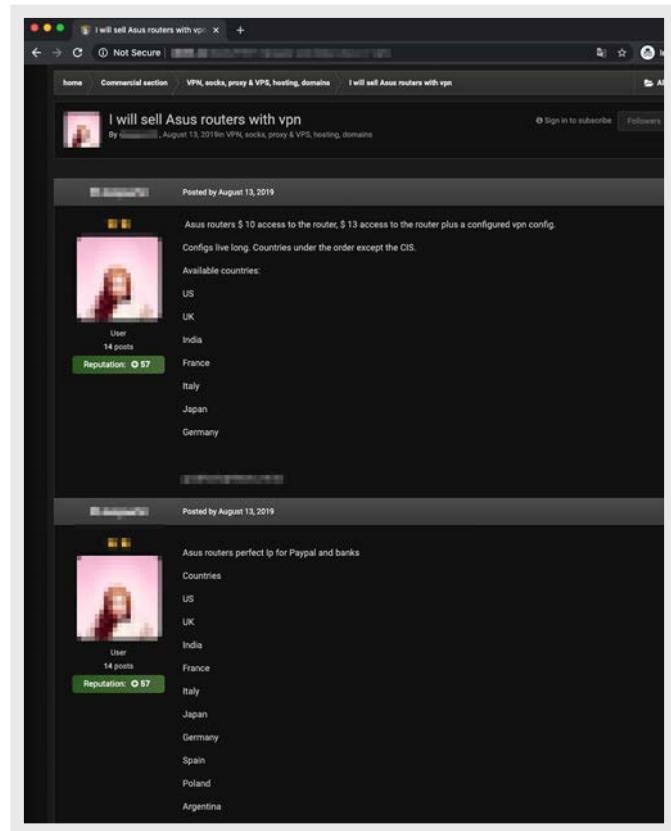


Figure 50. Compromised Asus routers sold as VPN nodes

In the case of a financial fraud investigation by law enforcement agencies, the owners of these compromised routers will probably be the first suspects. For law enforcement, it will often mean that all logs will be removed from IoT devices either immediately or during the next device restart cycle, making forensic investigation much more difficult.

IoT Devices as C&C Proxies for Botnets

“Professional-grade” botnets need to protect their core C&C infrastructure. For example, the Emotet botnet uses multiple layers of reverse proxies to protect their C&C infrastructure. In one of the confirmed cases, Emotet relayed their traffic through a Universal Plug and Play (UPnP) plugin of the routers,²⁷ confusing investigators by making the routers appear infected with Emotet.

This indicates that the occurrence of IoT devices in underground markets is increasing, and they are used not only for temporary actions like DDoS attacks but as part of mission-critical operations of mature underground actors. At the same time, this once again leaves the true owners of these compromised devices subject to the initial part of criminal investigations by law enforcement agencies.

Telephony-Related Services

The volume and type of telephony services sold in the underground demonstrate that the attackers are very familiar with telecom networks and the telecom infrastructure. While IP networks are a major component of hacker infrastructure, they are not the only component. We have also seen telephone numbers and telephony-related services being provided. The underground market has it all — from phone landing services and disposable phone numbers for SMS confirmation to checks and caller details on mobile phone numbers.



Figure 51. A screenshot showing offers of checks and subscriber details on mobile phone numbers

One of the most interesting services that we observed is a service for SMS phone confirmation and corporate email confirmation. This service allows attackers to easily create fraudulent accounts that can bypass commonly used verification approaches.

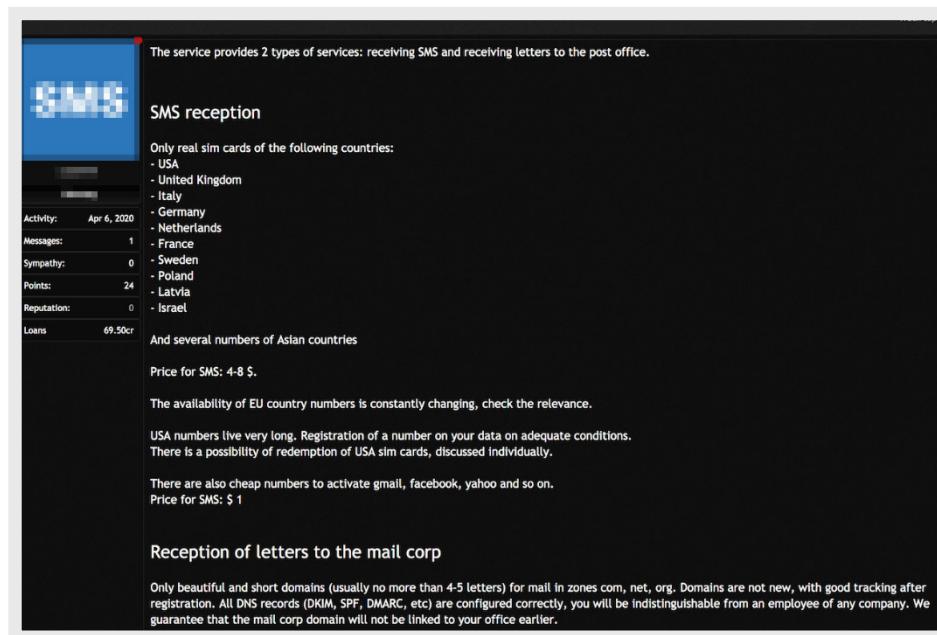


Figure 52. An advertisement offering SMS and email confirmation service for a fee

Route Hijacking, BGP, and Unused IP Space

Border Gateway Protocol (BGP) is used to exchange routing information between border routers of large internet providers and large organizations that need to manage their own IP space. Border gateway routing protocols are the core component of internet reliability as they are designed to dynamically reconfigure network routing traffic when some parts of the internet go offline. However, this feature comes at a price; such infrastructure is still vulnerable to human mistakes and even malicious actions.²⁸ Route misconfigurations and route leaks are common and could even partially lead to parts of the internet being subjected to outage or unreachability.²⁹

When exploited for malicious purposes, attackers can temporarily reroute some routes, as what happened with the MyEtherWallet Route 53 BGP hijack.³⁰ Attackers can also temporarily take over an unused IP space, start advertising routes for it, and use the space to conduct malicious activities like sending spam.³¹ The latter type of activity is more common as it does not directly cause any outages (no existing IP systems are taken over) and is significantly harder to trace.

One of the well-known incidents in this space was the takedown and boycott of Bitcanal,³² a Portuguese web hosting firm that was deliberately injecting routes via BGP³³ used to send spam.

Abuse of Satellite Infrastructure

Some highly sophisticated groups like Turla³⁴ use creative methods to hide their C&C machines via internet satellite links. Using such infrastructure, the attackers could inject packets from anywhere on the internet; as long as they can receive responses, they could conduct two-way communication between the infected machine and C&C. The receiving of the packets could be achieved in several ways; for instance, through temporal BGP route hijacking or hijacking of unused IP space, using a receive-only DVS-B satellite dish to receive signals or by compromising the ISP.

Receive-only satellite-based internet services are very common and have been widely available since the late 1990s in regions where cable-based last-mile internet could be an expensive investment due to low population density.

Many regional ISPs in Central Asia, the Middle East, and Africa have been using these technologies to optimize the cost of downstream traffic and provide cheaper internet access to rural and remote areas.³⁵ The outgoing traffic could be “injected” into the internet through an expensive cable link, while the responding traffic would be received over a cheaper satellite link.³⁶

Turla operators are likely very aware of these technologies as they reproduced the same architecture for their C&C operations. They may not even need to build their receiver but simply buy one from a service provider.

Conclusion

This research paper shows that the cybercrime infrastructure is a lot more developed and nuanced than the notion that the underground market is simply filled with “criminal servers for hire.” One could argue that the infrastructure element of cybercrime is one of the most mature aspects of the entire business. Cybercrime trends ebb and flow — network worms give way to trojans, browser exploits to spear-phishing attacks, theft-based business models to extortion-based ones — but through it all, the infrastructure underpinning it remains constant. Of course, it must also innovate, as shown in this research paper, but it is in a lower state of flux compared with the other areas of cybercrime.

This research paper continues from where we left off exploring the cybercrime infrastructure market and delved deeper into the technical side of its operations. We showed the common services you would expect to see deployed by almost every cybercrime business — right down to the more niche services deployed by specialist players in this ecosystem. We have shown that if a cybercriminal can imagine a need for an infrastructure offering, chances are good that a seller is already offering it, if not already thriving in a competitive market.

This research series concludes with part three, which looks into the ways some long-term criminal service providers sustain their operations. It will look into the factors that set them apart from their competition, the things they do to get repeat business from their regular customers, and the ways they evade arrest or disruption over extended periods. By detailing these factors, we hope to give investigators more insights that could help them take down these operations and apprehend the individuals behind them.

Cybercriminals need robust services that will last as long as possible without law enforcement disruption. This demand has spawned a whole industry of semi-legal services that cater to cybercriminals, indirectly aiding criminality. The challenge lies in the fact that offering robust, untraceable hosting services is not illegal on its own. Resolving this challenge is a very important piece of the puzzle for those tackling cybercrime as a global problem. Enacting laws to combat this industry is a strong step in the right direction.

At the start of this paper, we made a comparison between a cybercriminal enterprise and a traditional e-commerce business such as an online book store. While there are clear differences (i.e., a legitimate company does not need anonymity or bulletproof hosting), business owners — regardless if they’re running legitimate or criminal operations — ultimately look for the same thing when it comes to internet infrastructure: reliability and a range of services that address their business needs. This is something the criminal underground provides in abundance.

Appendix

Examining the Lifecycle of Compromised Server Assets

Compromised Server Kill Chain

This section examines the lifecycle of a typical compromised host. The diagram below shows three types of flows:

- Solid lines indicate the major flow from takeover to future monetization stages
- Dashed lines indicate optional flows — potential spinoffs and returns to the previous stages to highlight different monetization paths. These also highlight the fact that the same server can be monetized by several groups and resold many times, or that one criminal group can take over the server from another group and it will then follow yet another monetization path
- Dashed-and-dotted lines indicate an incident response (IR) team dealing with the threat

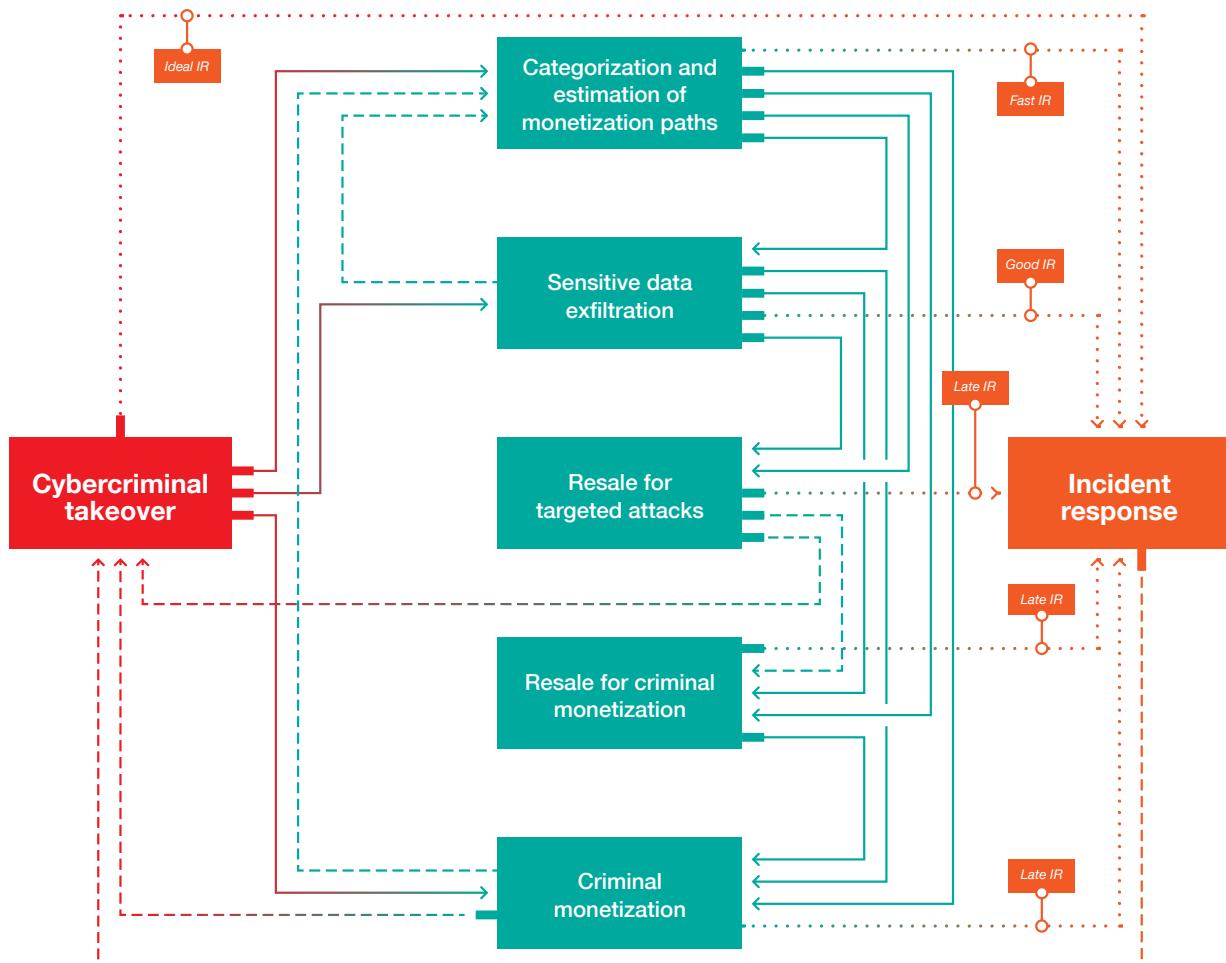


Figure 53. The monetization lifecycle of a compromised server

Each stage in the diagram is described in detail below.

Cybercriminal Takeover

Server takeover is the earliest stage of the lifecycle and usually includes several steps:

- Enumeration of exposed assets, which is normally done through network scanners
- Getting access to the asset
- Preliminary categorization of the asset

More precise techniques used to compromise servers are described in the “Compromised Machines Used as Dedicated Servers” section of this paper.

Criminal Approaches to Categorizing Assets

The underground market is service-oriented. One of the ways to understand the approaches that underground actors use to categorize compromised servers is to look into purchase orders in underground forums. Among other techniques, we used specific keywords that relate to “will buy dedicated server for [reason of purchase]” to find advertisements in underground forums that have been publicly indexed by search engines. The use of specific slang restricted search results to such underground forums only.

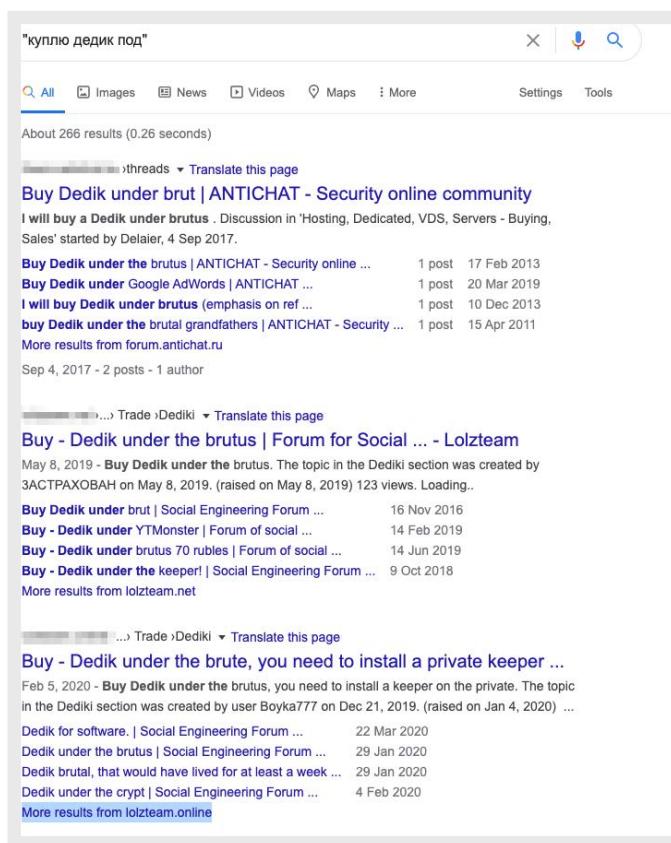


Figure 54. Search results of market requests for dedicated servers

Note: As machine translation was used, references to “buy dedic(ated server) under” should be considered as “buy dedic(ated server) for.”

Based on market requests, many sellers categorize their assets by features like performance (e.g., availability of GPU, bandwidth, CPU, memory, number of kernels, type of GPU, and type of storage). The type and speed of internet connection are very important for servers that are sold for brute-force attacks. Geographic location is an important criterion if servers are sold as proxies. The expected time of availability, in turn, becomes the warranty provided by the seller, usually measured in days and normally between one and 30 days.

These criteria are simple and can be automatically collected by software tools used by underground actors. Categorization at this level is much simpler for the infrastructure controllers, compared to the categorization that is done by mature sellers and buyers.

For more detailed categorization, actors use criteria related to potential restrictions on the use of the compromised server such as DNS, open ports, ping, WebRTC, and checks for flagging in public intelligence databases and blacklists.

The screenshot shows a forum post titled "Selling Dediks" in a dark-themed interface. The post discusses a server for sale, specifically a Dedik USA server located partly in Europe and some continents. It lists various configuration options and their costs:

- Cost:**
 - Win7.8 - \$ 5
 - Win10 - \$ 6
 - Server - \$ 3
 - Administrator rights + \$ 1
- Sampling:**
 - Available for selection by state / city (included in the price)
 - Sampling by ports + \$ 1
- Check:**
 - Check for Whoer and BlackList (included in cost)
- Check for proxy score and risk score:**
 - Risc Score / Proxy Score from 1 to 3 - win7.8 (\$ 6). From 0 to 1 - (\$ 7)
 - Win10 from 1 to 3 - (\$ 7). From 0 to 1 - (\$ 8)
- Warranty:**
 - Check Dedik within 30 minutes for validity and specified criteria.
 - 24 hours connection warranty.
 - Opportunity to purchase a Dedic with hidden accounting + \$ 1 to the set price, a 24-hour accounting guarantee.
- Contact me:**
 - Online from lunch until midnight Moscow time. Sunday-Friday, Saturday is a weekend off

Figure 55. A sample advertisement that mentions options for the operating system (OS), location, risk score checks, and their effect on pricing

Advanced categorization requires the collection of detailed information about compromised assets and their environment. Actions that are similar to the activity of legitimate IR teams carrying out attacker attribution are performed at this stage. This allows an attacker to understand exactly who their victim is. Actors can continue active actions such as analysis of installed software to understand the role of the server, analysis of the information stored on the server to decide if exfiltration is needed and if information can be resold separately, and scanning of nearby assets for lateral movement. Advanced categorization will be further discussed in the following sections.

After categorization, compromised assets are used or sold for particular purposes such as proxies, hosting services, or cryptocurrency mining. Cryptocurrency mining is usually done for monetization when the servers are idle (e.g., waiting for a buyer).

Sensitive Data Exfiltration

In underground forums, it is easy to find dumps of corporate emails, corporate and client databases, and confidential documents — the sort of data stored on servers that belong to organizations. The data exfiltration stage of monetization can happen after advanced categorization, when the attacker, even if their initial intent was to sell access to the server, discovers that stored data that is valuable enough to sell separately. Databases with credentials, personally identifiable information (PII), or financial information have a very high probability of being exfiltrated. The screenshot below shows an advertisement for a tool that does keyword-based searches for potential documents to be exfiltrated, including scanned documents in .jpg, .png, and .pdf format on the compromised server. As a result, this tool creates an archive of documents that match the search criteria.

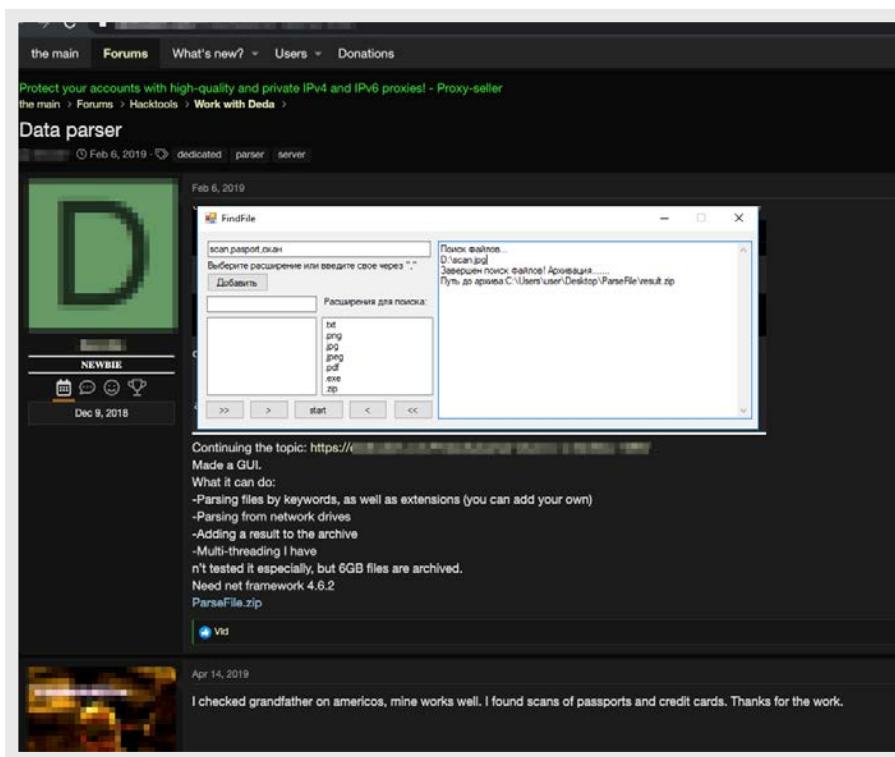


Figure 56. A tool for searching sensitive data on compromised servers

In the forum post following the advertisement, another actor confirmed that the tool worked well on a compromised server in the US. The tool was able to find scans of passports and credit cards.

The exfiltrated data can then be resold to different actors — even to actors with different specializations from the one who carried out the initial compromise. For instance, one actor may be looking for extracted credentials, while another is interested in PII or sensitive databases.



Figure 57. A request to buy dedicated servers with tax software in the US

Not all actors are mature enough to monetize the “hidden treasure” they get. Forum posts asking for advice on how to exfiltrate a particular type of information from compromised servers are also common.

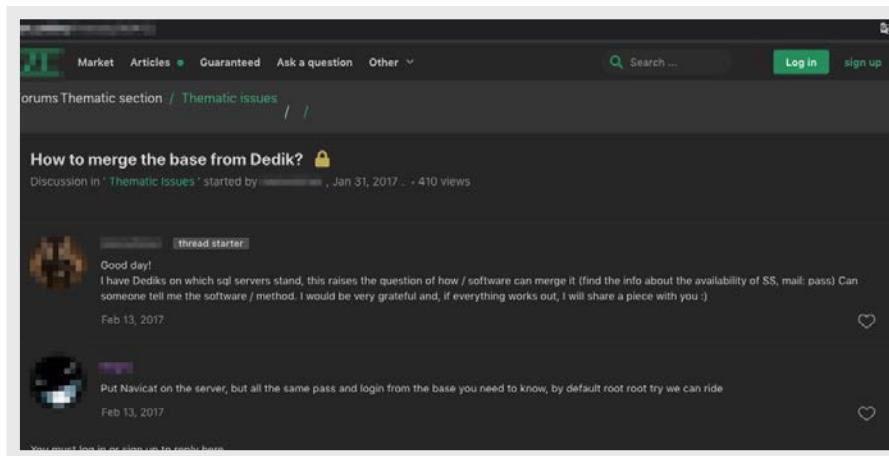


Figure 58. A request for help on information exfiltration from a compromised dedicated server

Resale for Targeted Attacks

If advanced categorization finds that servers may be of interest for actors focused on industrial espionage, these can be resold at a very high price, usually measured in thousands or tens of thousands of USD. These may be servers attributed to a particular organization or industry, containing PII or information related to finance, having specific geographical locations, or belonging to an organization on a group’s target list. For very sensitive assets that were compromised at scale, such as assets from large critical infrastructures of well-known companies, these can be sold in underground auctions with prices measured in hundreds of thousands of USD.

This operation is profitable for both the seller and the buyer. The seller can request a higher price, and the buyer can save time and often money (compared with the cost of carrying out their own attack). It also has an added advantage for the buyers since traces of initial compromise appear criminal, and they won’t be associated with the modus operandi of the more advanced attacker themselves.

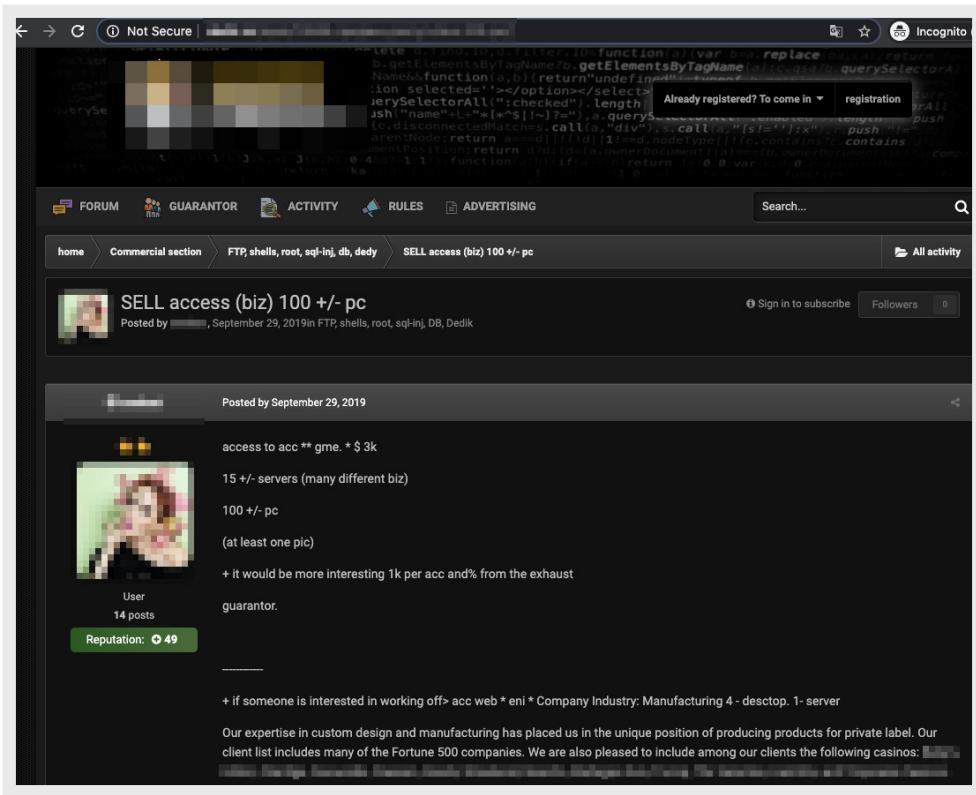


Figure 59. Sale of access to infrastructure with 15 servers and 100+ compromised PCs offered at US\$3,000. The footnote gives insights on the potential victim, indicating a strong candidate for a supply chain attack on several large casinos

This situation is very dangerous for infrastructure owners and has one of the worst possible outcomes from a compromise: an advanced targeted attacker could return the compromised asset to the underground market after carrying out their operation and offer it for sale for ransomware encryption. In this case, the targeted attacker can cover their tracks, and criminals will monetize the asset in another way.

Resale or Use for Criminal Monetization

Attackers in the underground have a variety of skill sets and capabilities. For larger criminal groups, it is possible to follow almost all parts of the monetization cycle alone, but others only want to be responsible for particular stages. They can buy “ready-to-go” products and optimally monetize them to best provide their “professional services” to other attackers. This is comparable to a large enterprise with many service offerings versus a smaller, niche player that excels in just a few.

This section combines two stages described in the diagram at the beginning of this appendix. The stages can cross each other many times during the monetization lifecycle.

It may surprise people to find that some of these more agile, niche players have even found a way to automate the monitoring and purchasing from sales threads for compromised servers. Based on our observation of underground forum offerings, we found that attackers have already adopted customized automated trading and monetization platforms, and seem to be actively using them. The example below

offers a platform that automates the processing of purchasing and monetizing compromised servers. They also mention that they are only interested in long-term collaboration with sellers, and only if the seller is capable of continually delivering more than a hundred compromised servers per day.

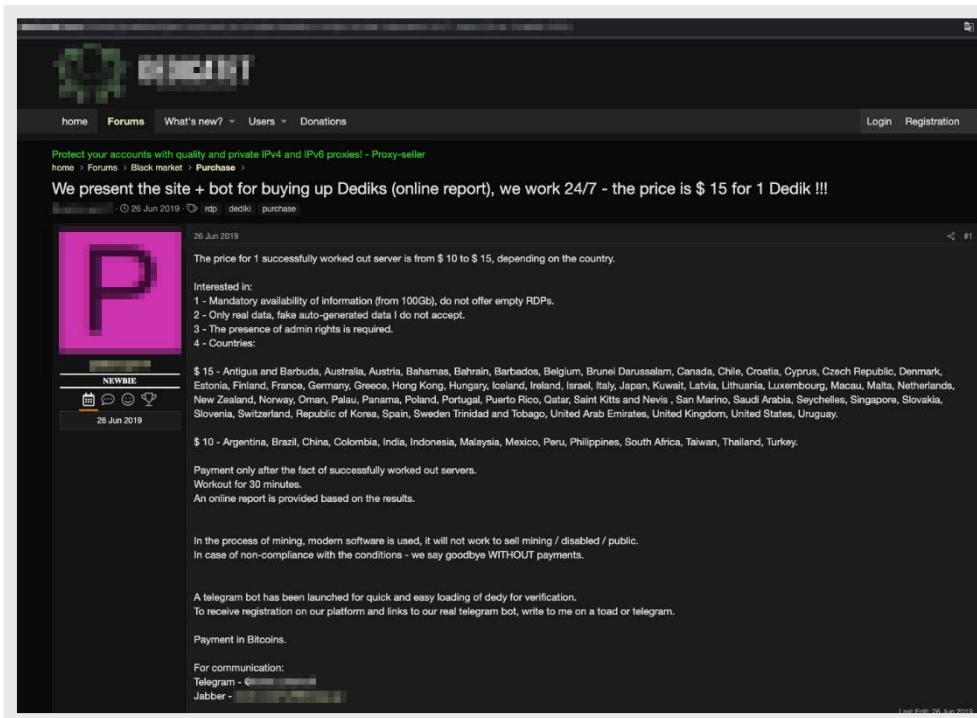


Figure 60. An advertisement offering a customized platform for purchase and monetization of compromised servers

Several techniques are used in further monetization stages. These techniques can be categorized according to their “visible immediate impact” to the infrastructure:

- **Low impact.** The monetization activity can last a long time and will not be visible to an asset owner with a non-mature security team. Monetization through cryptocurrency miners with proper setup falls into this category. If the mining does not consume all the system resources or if it only runs during idle times, it will barely be detected over time without proper tools. That’s why mining is often used as an intermediate stage while the current controller looks for a customer.
- **Medium impact.** The activity can periodically affect business processes and last an unpredictable period. This can range from several hours up to several years. The lifespan mostly depends on the activities of external security and IR teams. The periodical signals should be visible even with non-mature security teams. Mature IT teams will be present in IT and security logs. An example of medium impact would be a server monetized for hosting malicious services or for being a proxy. In this case, actors have the ability to adjust the use of resources on the compromised asset over time, but these activities can directly affect its lifespan. This means that over time, these servers will appear in public blacklists, threat intelligence feeds, and reports. An ISP can receive abuse reports from victims of attacks that can be traced to the compromised server and forwarded to the asset owner. This should be a very strong signal for the infrastructure owner to initiate incident response procedures.

- **High impact.** The activity is visible after a short period, not only to the asset security and IT teams but also to the business process owner. Depending on the impact, it could also be visible to the business owners. The next section provides an example of a high visible impact monetization scheme using targeted ransomware attacks.

Targeted Ransomware Attacks

Ransomware encryption is usually the last stage of underground monetization. By its nature, it exposes the fact of compromise to the asset owner; it's barely possible for other criminals to use the compromised server later, with some small exclusions. Attackers, for instance, can still run cryptocurrency-mining software on the compromised host or use it as a proxy during the ransomware attack while knowing that the service can be interrupted at any time.

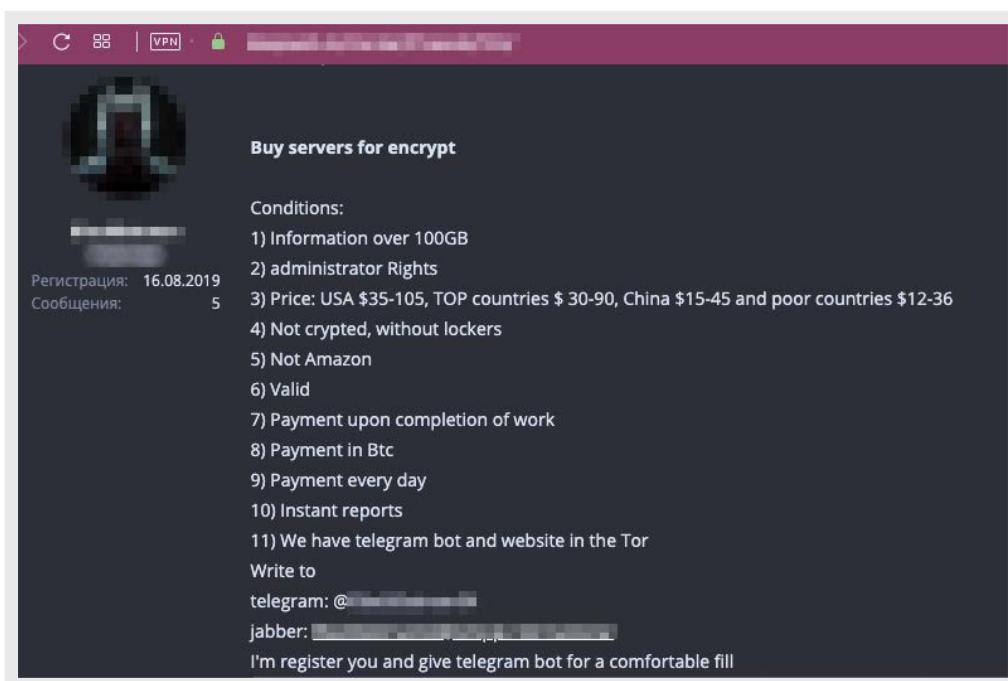


Figure 61. A request to buy compromised servers for ransomware encryption

The difference between targeted and mass ransomware attacks is in the potential impact and cost for the infrastructure owner. For mass ransomware campaigns, the price is usually fixed among targets. The price for targeted attack ransomware considers several factors:

- The attacker knows way more information about the infrastructure, and they know how to make a more significant impact and increase the chances for the ransom to succeed. In guides and discussions related to targeted ransomware campaigns in the underground, we observed recommendations on removing backup files and investigating if network-attached storage (NAS) devices are present in the network (and if they're possible to access and encrypt). Recommendations also included trying to compromise and encrypt other sensitive servers in the network.

- Attackers often have insights on local business processes and can choose the time when equipment outage can be most critical (e.g., when the company should submit tax reports to local authorities or during a key sales cycle).
- Attackers can set the ransom much higher compared to mass ransomware campaigns. In some cases, the ransom for compromised infrastructures can reach hundreds and thousands of USD.³⁷

Targeted ransomware attacks are visible and impactful, but the asset owner needs to keep in mind that this stage of the monetization kill chain may not be the stage that has the largest impact on their business. Ransomware monetization usually is one of the last stages of monetization for criminals. This means it's likely that the compromised asset has already experienced the earlier stages of compromise.

Definitions and Concepts

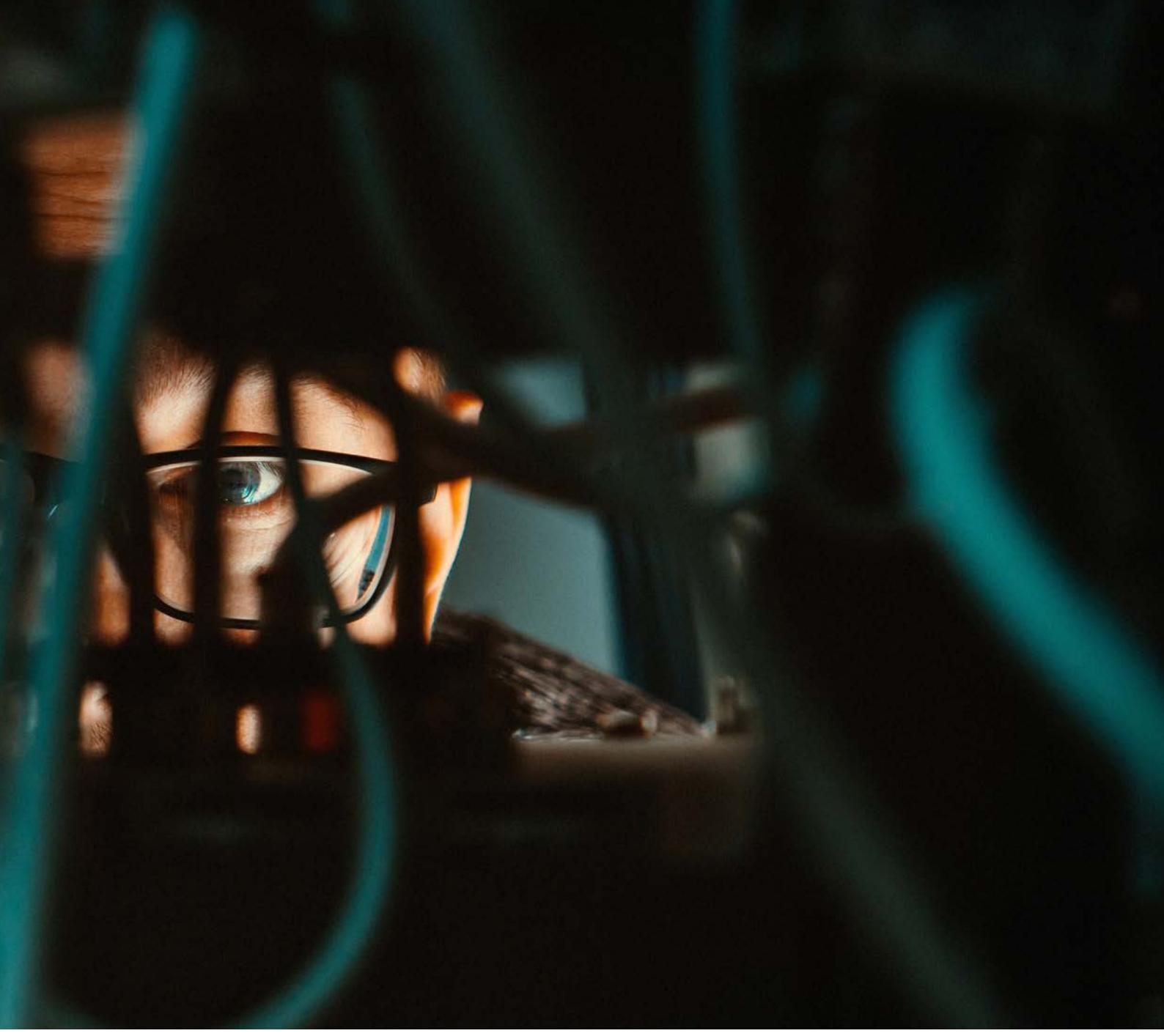
Here are several major concepts used throughout the paper, defined for the readers' benefit:

- **Bulletproof hosting** refers to several categories of hosting providers, including those who deliberately ignore abuse and legal requests, those who exist in countries with lax cybercrime laws, or even legitimate services with a poor abuse-handling record.
- **Dedicated hosting service, dedicated server, or managed hosting service** is a type of internet hosting whereby the client leases an entire server not shared with anyone else.
- **Domain generation algorithm (DGA)** is a computer program that generates domains to contact systematically or programmatically.
- **Fast flux** is a domain name service (DNS) obfuscation technique that botnets use to hide their servers behind an ever-changing network of compromised machines or proxies (See proxy.).
- **Internet service provider (ISP)** is an organization that provides services for accessing or using the internet.
- **Peer-to-peer** refers to infrastructure that operates as a network of computers, with each acting as a server to others, sharing access to files or network traffic without the need for a central server. This is often seen in VPN setups.
- **Proxy** is a computer that functions as a relay between a client and a server, offering a degree of obfuscation of the client's true location. One well-known type uses a protocol known as SOCKS.
- **Remote Desktop Protocol (RDP)** is a protocol developed by Microsoft that provides a user with a graphical interface for a computer being connected across a network. Virtual network computing (VNC) is a similar standard.
- **Time to live (TTL)** is the amount of time a domain to IP mapping will be cached (reused) by a computer before requesting a new IP resolution. Short TTLs are used by fast-flux botnets that seek to alternate the IP behind a domain regularly.
- **Traffic Direction System (TDS)** uses a network of connected landing pages or servers that direct internet traffic to its ultimate end goal based on a variety of criteria such as geographic location, operating system, browser, and language.
- **Virtual private network (VPN)** is a private network overlaid virtually on top of a public network such as the internet.
- **Virtual private server (VPS)** is a virtual machine sold as a service by an internet hosting provider.

References

- 1 Vladimir Kropotov, Robert McArdle, and Fyodor Yarochkin. (Jul. 21, 2020). *Trend Micro Security News*. “Hacker Infrastructure and Underground Hosting 101: Where Are Cybercriminal Platforms Offered?” Accessed on Aug. 4, 2020 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hacker-infrastructure-and-underground-hosting-101-where-are-cybercriminal-platforms-offered>.
- 2 Associated Press. (Jul. 16, 2019). *Yahoo! Finance*. “Ukrainian hacker sought by US arrested.” Accessed on Jun. 30, 2020 at <https://finance.yahoo.com/news/ukrainian-hacker-sought-us-arrested-152808009.html>.
- 3 The MITRE Corporation. (n.d.). *MITRE*. “Brute Force.” Accessed on Jun. 30, 2020 at <https://attack.mitre.org/techniques/T1110/>.
- 4 Vladimir Kropotov, Robert McArdle, and Fyodor Yarochkin. (Jul. 21, 2020). *Trend Micro Security News*. “Hacker Infrastructure and Underground Hosting 101: Where Are Cybercriminal Platforms Offered?” Accessed on Aug. 4, 2020 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hacker-infrastructure-and-underground-hosting-101-where-are-cybercriminal-platforms-offered>.
- 5 Trend Micro. (Apr. 30, 2020). *Trend Micro Security News*. “Security 101: How Fileless Attacks Work and Persist in Systems.” Accessed on Jun. 30, 2020 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-how-fileless-attacks-work-and-persist-in-systems>.
- 6 Paul Pajares, Augusto Remillano II, Don Ovid Ladores, and Franklyn Uy. (Mar. 31, 2020). *Trend Micro*. “Raccoon Stealer’s Abuse of Google Cloud Services and Multiple Delivery Techniques.” Accessed on Jun. 30, 2020 at <https://blog.trendmicro.com/trendlabs-security-intelligence/raccoon-stealers-abuse-of-google-cloud-services-and-multiple-delivery-techniques/>.
- 7 Falcon Sandbox. (Dec. 23, 2019). *Hybrid Analysis*. “d21ebbc03f3bd1b185a6d933e6865a63914aacdeed3304610f5180cf9014b2.exe.” Accessed on Jun. 30, 2020 at <https://www.hybrid-analysis.com/sample/d21ebbc03f3bd1b185a6d933e6865a63914aacdeed3304610f5180cf9014b2?environmentId=100>.
- 8 Thaddeus E. Grugg (2015). *Grugg*. “Hacker OPSEC.” Accessed on Jun. 30, 2020 at <https://grugg.github.io/>.
- 9 Augusto Remillano and Kiyoshi Obuchi. (Mar. 12, 2019). *Trend Micro*. “From Fileless Techniques to Using Steganography: Examining Powload’s Evolution.” Accessed on Jun. 30, 2020 at <https://blog.trendmicro.com/trendlabs-security-intelligence/from-fileless-techniques-to-using-steganography-examining-powloads-evolution/>.
- 10 Aliakbar Zahravi. (Dec. 14, 2018). *Trend Micro*. “Cybercriminals Use Malicious Memes that Communicate with Malware.” Accessed on Jun. 30, 2020 at <https://blog.trendmicro.com/trendlabs-security-intelligence/cybercriminals-use-malicious-memes-that-communicate-with-malware/>.
- 11 Vladimir Kropotov and Fyodor Yarochkin. (Sep. 28, 2017). *Trend Micro*. “Business Process Compromise and the Underground’s Economy of Coupon Fraud.” Accessed on Jun. 30, 2020 at <https://blog.trendmicro.com/trendlabs-security-intelligence/business-process-compromise-underground-coupon-fraud/>.
- 12 Trojan-GFW. (n.d.). *GitHub, Inc.* “Trojan-GFW.” Accessed on Jun. 30, 2020 at <https://github.com/trojan-gfw>.
- 13 ValdikSS. (Nov. 1, 2019). *GitHub, Inc.* “ValdikSS/GoodbyeDPI.” Accessed on Jun. 30, 2020 at <https://github.com/ValdikSS/GoodbyeDPI>.
- 14 Boxun. (May 15, 2019). *Boxun*. “翻墙技术员孙东洋被抓事件详情:以黑客名义被起诉.” Accessed on Jun. 30, 2020 at <https://boxun.com/news/gb/china/2019/05/201905150940.shtml>.
- 15 斯影. (Jan. 11, 2019). *BBC*. “中国VPN用户被罚“翻墙”怎么会违法.” Accessed on Jun. 30, 2020 at <https://www.bbc.com/zhongwen/simp/chinese-news-46823319>.
- 16 Katmagic. (Jun. 29, 2012). *GitHub, Inc.* “katmagic/Shallot.” Accessed on Jun. 30, 2020 at <https://github.com/katmagic/Shallot>.
- 17 GReAT. (Aug. 23, 2018). *Securelist*. “Operation AppleJeus: Lazarus hits cryptocurrency exchange with fake installer and macOS malware.” Accessed on Jun. 30, 2020 at <https://securelist.com/operation-applejeus/87553/>.
- 18 Trend Micro. (Oct. 25, 2019). *Trend Micro Security News*. “Phishing Campaign Targets Humanitarian and Other Non-Governmental Organizations.” Accessed on Jun. 30, 2020 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/phishing-campaign-targets-humanitarian-and-other-non-governmental-organizations>.
- 19 Robert McArdle and David Sancho. (Nov. 19, 2013). *Trend Micro Security News*. Accessed on Jun. 30, 2020 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/bit-domain-deliver-malware-and-other-threats>.

- 20 John Kuhn. (Jul. 18 2018). *IBM Security*. “Gandcrab Ransomware Walks its Way onto Compromised Sites.” Accessed on Jun. 30, 2020 at <https://exchange.xforce.ibmcloud.com/collection/Gandcrab-Ransomware-Walks-its-Way-onto-Compromised-Sites-a0c4a4b58832c050569ae0d5cd3a5549>.
- 21 Nick Biasini, Nick Lister, and Christopher Marczewski. (May 9, 2018). *Cisco Talos Intelligence*. “Gandcrab Ransomware Walks its Way onto Compromised Sites.” Accessed on Jun. 30, 2020 at <https://blog.talosintelligence.com/2018/05/gandcrab-compromised-sites.html>.
- 22 MingYen Hsieh, CH Lei, and Kawabata Kohei. (Nov. 6, 2017). *Trend Micro*. “ChessMaster’s New Strategy: Evolving Tools and Tactics.” Accessed on Jun. 30, 2020 at <https://blog.trendmicro.com/trendlabs-security-intelligence/chessmasters-new-strategy-evolving-tools-tactics/>.
- 23 Abraham Camba and Janus Agcaoili. (Apr. 19 2018). *Trend Micro*. “XTRAT and DUNIHI Backdoors Bundled with Adwind in Spam Mails.” Accessed on Jun. 30, 2020 at <https://blog.trendmicro.com/trendlabs-security-intelligence/xtrat-and-dunihi-backdoors-bundled-with-adwind-in-spam-mails/>.
- 24 Bartblaze. (Aug. 28, 2017). *Alienvault, Inc.* “Adwind: A Cross-Platform RAT.” Accessed on Jun. 30, 2020 at <https://otx.alienvault.com/pulse/59a41117959360468cde5908>.
- 25 Fernando Mercês. (May 2, 2018). *Trend Micro*. “Cryptocurrency-Mining Malware Targeting IoT, Being Offered in the Underground.” Accessed on Jun. 30, 2020 at <https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-mining-malware-targeting-iot-being-offered-in-the-underground/>.
- 26 Stephen Hilt et al. (Sep. 10, 2019). *Trend Micro Security News*. “Uncovering IoT Threats in the Cybercrime Underground.” Accessed on Jun. 30, 2020 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-internet-of-things-in-the-cybercrime-underground>.
- 27 Sergiu Gatlan. (Apr. 25, 2019). *BleepingComputer*. “Emotet Uses Compromised Devices as Proxy Command Servers.” Accessed on Jun. 30, 2020 at <https://www.bleepingcomputer.com/news/security/emotet-uses-compromised-devices-as-proxy-command-servers/>.
- 28 Louis Poinsignon. (Apr. 17, 2020). *Cloudflare*. “Is BGP Safe Yet? No. But we are tracking it carefully.” Accessed on Jun. 30, 2020 at <https://blog.cloudflare.com/is-bgp-safe-yet-rpki-routing-security-initiative/>.
- 29 MANRS. (Apr. 6, 2020). *MANRS*. “Not just another BGP Hijack.” Accessed on Jun. 30, 2020 at <https://www.manrs.org/2020/04/not-just-another-bgp-hijack/>.
- 30 Aftab Siddiqui. (Apr. 27, 2018). *Internet Society*. “What Happened? The Amazon Route 53 BGP Hijack to Take Over Ethereum Cryptocurrency Wallets.” Accessed on June. 30, 2020 at <https://www.internetsociety.org/blog/2018/04/amazons-route-53-bgp-hijack/>.
- 31 Pierre-Antoine Vervier and Olivier Thonnard. (Feb. 1, 2013). *EURECOM*. “SpamTracer: How Stealthy Are Spammers?.” Accessed on Jun. 30, 2020 at <http://www.eurecom.fr/en/publication/3919/download/rs-publi-3919.pdf>.
- 32 Brian Krebs. (Jul. 11, 2018). *Krebs on Security*. “Notorious ‘Hijack Factory’ Shunned from Web.” Accessed on Jun. 30, 2020 at <https://krebsonsecurity.com/2018/07/notorious-hijack-factory-shunned-from-web/>.
- 33 Richard Chirgwin. (Jul. 11, 2018). *The Register*. “BGP hijacker booted off the Internet’s backbone.” Accessed on Jun. 30, 2020 at https://www.theregister.com/2018/07/11/bgp_hijacker_booted_off_the_internets_backbone/.
- 34 Stefan Tanase. (Sep. 9, 2015). *Securelist*. “Satellite Turla: APT Command and Control in the Sky.” Accessed on Jun. 30, 2020 at <https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/>.
- 35 BusinessCom Networks. (n.d.). *BusinessCom Networks*. “Satellite Internet in Kazakhstan.” Accessed on Jun. 30, 2020 at <https://www.bcsatellite.net/satellite-internet-in-kazakhstan/>.
- 36 Hajid. (Jul. 13, 2006). *MikroTik*. “Satellite Downstream only and FO Connection.” Accessed on Jun. 30, 2020 at <https://forum.mikrotik.com/viewtopic.php?t=9634>.
- 37 Ionut Ilascu. (Jun. 26, 2019). *BleepingComputer*. “Attackers Earn Over \$1 Million in Florida Ransomware Attacks.” Accessed on Jun. 30, 2020 at <https://www.bleepingcomputer.com/news/security/attackers-earn-over-1-million-in-florida-ransomware-attacks/>.



TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

