U-Markt
Peering into the German Cybercriminal Underground

Forward-Looking Threat Research (FTR) Team
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.

Contents

4
Market landscape

13
German underground market offerings

20
Only in Germany

36
German and Russian underground overlaps
The German cybercriminal underground is well-developed and -managed by cybercriminals even though it remains a small community in number compared with the Russian\(^1\) and Brazilian\(^2\) underground markets. It may also be the most developed underground within the European Union (EU) despite the existence of a French underground market. The Spanish underground, however, merged with the Latin American market.

In the German underground, we find a mixed bag of cybercriminal products and services that include crimeware, credentials, fake items, and drugs. Interestingly, it has a similar structure to the Deep Web\(^3\); it seems to offer as much as possible to stay up. This could be due to some limitations like language barrier and the market’s overall size.

The German underground is indeed a newcomer that offers everything cybercriminals need to start in the cybercrime business. It specifically caters to a regional market, as its offerings (Packstation services; hacked accounts for dropping; German, Austrian, and Swiss credit card and financial account credentials; and malware developed by German coders) would most appeal to German speakers.

This paper focuses on three main areas—the major forums and marketplaces in the German underground, the unique wares only seen in these forums, and how the German compares with the Russian market. It features the product and service offerings in the market so you can better understand its dynamics. We also chose to feature a specific marketplace to clearly show what wares are sold, how much it sells, and how it operates.

Special attention was also paid to wares unique to German forums. These include Packstation services as new dropping means and locally produced crimeware (tools programmed and sold). We also compared the German with the Russian underground, mostly because the latter is the most significant and relevant environment to the former. We looked at connections that German underground players have forged with their Russian counterparts, along with the unsurprising ways they seem to have been collaborating.
SECTION 1

Market landscape
Market landscape

Market structure

Underground environment
The German underground’s infrastructure does not really differ from that of other markets and even typical German forums. We determined German underground forums not only by the language participants used but also based on their targets’ geographical location. Germany as a country is less isolated from the global business infrastructure than Russia or China. As such, it is more difficult to identify whether a cyber activity associated with it belongs to the German underground or is more global in nature.

The actual number of German forums and marketplaces is small but the forum user volume is relatively significant and gives a clear idea on ongoing cybercriminal activities. Note that forum user volume is easier to track than actual marketplace activities. We saw 10 major forums and at least two marketplaces that do not only specialize in selling crimeware but also drugs, fakes, and other illegal wares. We found almost 70,000 users registered in German underground forums. At least 20,000 users have posted at least once on a German underground forum, which could indicate room for future growth. We counted the number of active users based on publicly available parsed information.

Research challenges
One of the reasons why researchers do not really take a closer look at specific EU countries lies in the scope of underground forums and related activities. English is the main language in the cybercrime scene, much as it is the international means of communication. As such, a wide variety of products are offered on English forums and marketplaces, which makes doing business on a German platform very challenging. Competition comes not only from English marketplaces but also from better-known communities like the Russian underground. German cybercrime business owners and site developers need to create a niche and provide customized content (fraud schemes, drugs, credit cards) that cater to the local market. The German market players’ main focus has been to overcome these challenges in creative ways, providing interesting findings on local cybercriminal activities.
Underground forums and marketplaces

The German underground, much like its foreign counterparts, comprises forums and marketplaces. While forums serve as the main venue for introductions and information exchange, they also serve as the go-to place for special, sometimes customized, items. These marketplaces exclusively function as a place for trading goods like local credit cards, hacked accounts, and fakes. They also serve as cybercriminal wannabes’ first point of entry into the underground.

We often find ads for partner sites in the form of banners. German underground marketplaces are sometimes incorporated into or connected to forums. But there are also separate sites that only serve as marketplaces. A distinguishing characteristic between independent marketplaces and those owned by forums is that the latter get heavily advertised via banners.

We found five main forums described in more detail below.

<table>
<thead>
<tr>
<th>Marketplace/Forum</th>
<th>Access</th>
<th>Offerings</th>
<th>Total number of registered users</th>
<th>Active since</th>
<th>Number of active users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bus1nezz.biz</td>
<td>Closed forum with restricted access</td>
<td>Crimeware, drugs/narcotics</td>
<td>6,200</td>
<td>2011</td>
<td>1,580</td>
</tr>
<tr>
<td>Secunet.cc</td>
<td>Security forum with both publicly accessible and restricted-access areas</td>
<td>Hacking tools, stolen account credentials</td>
<td>1,800</td>
<td>2013</td>
<td>650</td>
</tr>
<tr>
<td>Back2hack.cc</td>
<td>Security forum with both publicly accessible and restricted-access areas</td>
<td>Security wares</td>
<td>9,346</td>
<td>2008</td>
<td>1,440</td>
</tr>
<tr>
<td>German-plaza.cc</td>
<td>Marketplace that requires user registration (username and password are required for entry) but activation is automatic</td>
<td>Stolen credit card and account credentials, server access</td>
<td>Not available</td>
<td>2015</td>
<td>Not available</td>
</tr>
<tr>
<td>Crimenetwork.biz</td>
<td>Forum with tiered access</td>
<td>Crimeware, drugs/narcotics</td>
<td>64,000</td>
<td>2009</td>
<td>8,000</td>
</tr>
</tbody>
</table>

Table 1: Main forums/marketplaces found in the German underground
Bus1nezz.biz

Bus1nezz.biz is a closed underground forum with a standard set of offerings that include cybercrime tools and real-world items like drugs and narcotics. It is hosted on CloudFlare, a domain registrar based in China. To date, it has around 6,500 registered users, at least 1,520 of whom are considered active or regularly post on the forum. The forum has been active since 2011 and has since amassed 12,179 topics and 50,986 posts. Some noteworthy bus1nezz.biz content include posts on escrow or “treuhand” services; a “vendor marktplatz”; a “4free area”; a “tool area” where users can buy remote access tools (RATs), crypters, binders, and stealers; and coding, fraud, and hacking areas.

Figure 1: Bus1nezz.biz’s home page with banner ads for vanille.cc (a stolen credit card marketplace) and secureVPN.to (a virtual private network [VPN]) service provider, along with top 20 statistics on the most relevant news and updates
Secunet.cc, active since 2013, is a publicly accessible underground forum hosted by OVH, a hosting service provider based in France. It has 2,226 users, 2,432 topics, and 13,381 posts. It poses as a cybersecurity information forum where users can discuss white-hat matters but also serves as a distribution platform for malware or hacked accounts. Users can easily find and download RATs, Trojans, password stealers, and the like or acquire hacked Zalando.de, Deezer Zevera, and other accounts from it. Though it poses as a security board, secunet.cc offers a decent array of cybercriminal desirables.
Like secunet.cc, back2hack.cc also poses as a security board. It has both publicly accessible and restricted-access areas and is hosted on OVH. To date, it has 16,658 registered users, at least 1,440 of whom are considered active; 6,420 topics; and around 41,000 posts.
Crimenetwork.biz

Crimenetwork.biz is the biggest German underground forum with 60,000 registered users. Though not every user is active, its huge user base is enough indication of its size. It gets several thousand visits on a daily basis. It has a more obvious user hierarchy, as evidenced by varying user levels ranging from simple members to escrow agents and vendors.

![Figure 4: Crimenetwork.biz’s user levels](image)

Crimenetwork.biz has several affiliate marketplaces like chemical-love.cc that sell drugs. Affiliation, in this context, was determined based on the ads seen in the main forum. As such, crimenetwork.biz most likely also controls and owns chemical-love.cc.

![Figure 5: Crimenetwork.biz’s home page](image)
German-plaza.cc

German-plaza.cc is an underground marketplace hosted on CloudFlare. It offers stolen credit cards and accounts (retail and online banking) and is structured like an online shop.

![German-plaza.cc](image)

**Figure 6:** German-plaza.cc offers scanned identification (ID) cards

Banner ads

Banner ads are an easy way to promote partner sites (a marketplace run by those behind a certain forum in any community, most notably in the Russian underground). These can help marketplaces widen their client bases.

1. ![Kokain/SPEED/Ketamin](image)
2. ![Chemical Love](image)
3. ![Dumps and Cards](image)
4. ![Perfect Hausdrop Tutorial](image)
5. ![Http://2force.cn](image)
6. ![Mailstore.cc](image)

**Figure 7:** Banners 1 and 2 are animated frames that takes users to chemical-love.cc, the biggest drug marketplace on crimenetwork.biz; banner 3 takes users to Russia’s biggest bulletin board for stolen credit cards, Rescator.CC, access to which is only granted to invitees or referrals; banner 4 takes users to forum sections on dropping and Packstation services; banner 5 takes users to a carding domain; banner 6 takes users to a spamming service provider (1,000 email addresses for €1.50 [US$1.60])

---

* Currency exchange rate as of 18 November 2015 was used throughout this paper (US$1 = €0.94)
Restricted-access areas

The online black market typically offers tiered access. It has areas that require user credentials so they can go deeper and those that are publicly accessible. Users with substantial skills, connections, or know-how can obtain the highest access level but only after going through a vetting process. Those with low access levels mostly operate in open forums or forum sections with relatively minimal entry barriers.

The underground forums featured here offer varying access levels to sensitive information published by their users. Some (bus1nezz.biz) are by-invitation only and as such require administrator approval. Others only require registration. This is where intraforum dynamics come into play. In some forums, one needs to know other members before getting invited. On back2hack.cc, for instance, users need to make a sound impression and get informally “accepted” before they can see more information. Those who do not make the cut can only access certain areas. Some new registrants make an impression with meaningful posts. These posts increase their ranking in terms of reliability, value, and contribution that in turn gets them access to more relevant forum content.

The Deep Web and .onion mirrors

The German underground does not have a clear tiered structure. This makes Deep Web locations more difficult to access. There are, however, forums that can be reached via The Onion Router (TOR). These are .onion mirrors and not separate sites. Several of the featured forums use .onion mirrors for users who put a premium on their anonymity. Those who wish to conceal their illicit activities can also use proxies or anonymized VPNs. Users who do not feel safe accessing forums openly have Deep Web options. They normally do not want to disclose their Internet Protocol (IP) addresses or be tracked by investigators.

Interestingly, the Russian underground does not offer this kind of access layer. Even the most popular Russian underground forums do not use the Deep Web. This could likely be due to stricter law enforcement monitoring in Germany. Using .onion mirrors can slow down transactions but that’s an inconvenience German cybercriminals are willing to accept.

<table>
<thead>
<tr>
<th>Forum/Marketplace</th>
<th>.Onion mirror</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bus1nezz.biz</td>
<td>Bizznza4vtgdsdrbg.onion</td>
</tr>
<tr>
<td>Black2hack.cc</td>
<td>Gerpla4lgmngtpgw.onion</td>
</tr>
<tr>
<td>German-plaza.cc</td>
<td>Gerpla4lgmngtpgw.onion</td>
</tr>
<tr>
<td>Crimenetwork.biz</td>
<td>Crimenc5wxi63f4r.onion</td>
</tr>
</tbody>
</table>

*Table 2: Featured forums’/marketplaces’ .onion mirror sites*
German underground market offerings
German underground market offerings

The German underground does not have as wide a selection of offerings as the Russian market. In most cases, it isn’t necessary to search for special goods and services in local communities because global (English-speaking) markets have more to offer. But when it comes to customized wares, it is harder to find appropriate equivalents. This is a niche that smaller communities (like the German underground) need to find in order to thrive and stay up.

The German underground is not as strong as the Russian market with regard to crimeware. Its main offerings include fake IDs, stolen credit cards, data dumps, and hacked accounts. But like any other fully functioning underground market, it also offers concealment methods and infrastructure in the form of bulletproof hosting, proxy, and VPN services.

Every cybercriminal scheme in Germany involves monetizing stolen credit cards, dropping, and stealing online account credentials. We saw a new dropping scheme specific to the German environment that does not need actual droppers and uses fake deliveries instead by exploiting the German postal service, Packstation.

BPHSs

Bulletproof hosts serve as hideouts for malicious content and the foundation of any cybercriminal operation. The same is true in the German underground. Bulletproof hosts are used to store malware components, exploit kits, and the like. They can also serve as botnet command centers; stolen data repositories; and phishing, pornographic, or scam site hosts. Most bulletproof hosting service (BPHS) providers feign legitimacy but allow the conduct of malicious activities and so operate in countries with lax laws to evade litigation. They usually abide by one of three business models:
• **Model 1: Dedicated bulletproof servers:** BPHS providers create a convincing business front to evade law enforcement suspicion. They usually cater to customers who need to host content that may be considered illegal in certain countries.

• **Model 2: Compromised dedicated servers:** BPHS providers choose to compromise dedicated servers and rent these out to parties who wish to host malicious content.

• **Model 3: Abused cloud-hosting services:** Cybercriminals abuse cloud-hosting services like Amazon Web Services (AWS), Hetzner, OVH, and LeaseWeb to host command-and-control (C&C) servers or drop stolen data, among other malicious purposes. These services are abused without their owners’ knowledge.

BPHS providers in the German underground typically adhere to models 2 and 3 because creating a hosting environment in the face of strict laws is hard to do. None of the German underground forums are hosted in the country or the EU. The featured forums and marketplaces use content proxy services like CloudFlare. To evade local authorities, the forums’ domain names are not registered in Germany or the EU. These mostly use extensions like .cc and are hosted in Asia (Hong Kong or Vietnam).

These reasons support why the reselling option is most favored and discussed on forums. Most German underground forum members use Russian- or Ukrainian-controlled BPHSs like 2x4.ru, hosting.ua, infiniumhost.ru, anders.ru, and bulletproof-web.ru.

![Figure 8: Crimenetwork.biz discussion on hosting a botnet that points users to Russian hosts, infiniumhost.ru, bulletproof.web.ru, and the like](image)

German underground forums feature dozens of Russian BPHS resellers. Users can directly contact and them and avail of their services once payment is made. Resellers fulfill more of an advisory function and offer more detailed information via private messaging. They are not the actual BPHS owners but German-speaking resellers who have carved out niches in the local underground community. Most users buy from global players like those in the Russian underground. A few authentic German BPHS providers exist but they face stiff competition from bigger and better-known players. They typically have servers in the Netherlands, which has laxer laws compared with other EU countries, though their service prices and locations largely depend on the risks involved in hosting users’ desired content.
Figure 9: Crimenetwork.biz BPHS offerings (dedicated-denial-of-service- [DDoS]-protected virtual server hosting, €11+ [US$11.73+], depending on configuration; dedicated server hosting, starting at €55 [US$58.65]; and fast flux services, which are typically used for phishing and spamming, as these use a predefined set of domain names that are periodically rotated to hide C&C server IP addresses)

In the screenshot above, a user offers hosting services in crimenetwork.biz. He also offers support via email and individual consultations to customers in search of specific configurations. He offers a special price for fast flux services, which are typically not offered in the German underground. This indicates that he is still trying to establish himself as a hosting vendor in the market.
Fake IDs

A relatively huge chunk of the German underground caters to producing and selling fake IDs, including passports and driving licenses. Clients in search of such usually need noncontact fake identities to register for Packstation or other similar services. Others are trying to fake their ages or creating new personas. Reselling scanned copies of actual IDs is common. These fakes are used to open bank accounts or obtain additional information for more intricate social engineering scams. Overall, the demand for such items is big in the German underground, as evidenced by the number of sites that advertise them.

Figure 10: Ad for real driving licenses, IDs, and passports from Roy’s documents; IDs can be customized, depending on clients’ specifications

Figure 11: Post that sells scanned ID copies, some of which have been verified with vendors and 60% remain unused (male IDs cost €10 [US$10.66] worth of bitcoins each, female IDs cost €8 [US$8.53] worth of bitcoins each)
Figure 12: Profile picture of Sandmann, a popular fake ID seller on crimenetwork.biz

Figure 13: Sandmann’s fake ID offerings
Hacked accounts

Though some German underground forum users sell hacked accounts, others give them away for free, something we haven’t seen in the Russian market. These include Sky TV, Netflix, Amazon, and Zalando accounts. Giving these away could be a means to please other community members in hopes of building up one’s reputation or in exchange for connections or help in other areas.

Hacking accounts is after all not hard to do. Usual means to do so include phishing and brute forcing. Users can easily configure a botnet to extract desired information from infected machines. This can be done by infecting browsers, using keyloggers or screenshot capturers, or stealing browser cookies—all basic tasks that can be accomplished with standard cybercrime tools. They can also steal email accounts, which are usually connected to other online accounts, giving them a means to get as much information as they need to further their nefarious causes.

Hacked accounts can be used for dropping or simply sold. Stealing someone’s Amazon or Zalando account not only gives cybercriminals access to the victim’s username and password but also to his credit card and other personal information. The stolen information can then be used for all kinds of fraudulent transactions.

Netflix accounts, which cannot be easily resold because buyers will not be able to use video-on-demand accounts tied to private identifiable IP addresses, are mostly used for dropping or given away for free.

Crypting services

Crypting allows cybercriminals to hide their creation’s malicious routines by packing (crypting) a piece of malware using a variety of techniques. Crypting services abound in the German underground.

Figure 14: Post selling HyperText Transfer Protocol (HTTP) and Internet Relay Chat (IRC) bots, RATs, and crypters
SECTION 3

Only in Germany
Only in Germany

Payment, escrow, and dropping services

Treuhand
As in most underground environments, escrows (“treuhand” in the German underground) act as middlemen between buyers and sellers. In the underground, there is no legal way to make claims as in the real world. As such, escrows are needed to ensure smooth business transactions. Escrows process transactions for a certain fee, typically 3–15% of the amount that needs to be paid. Upon receiving this fee, escrows hand the payment to the seller and the goods bought to the buyer.

Bitcoins are the preferred mode of payment in the German underground but some sellers prefer to get paid in vouchers or “gutscheine.” Getting paid in vouchers or online shop gift cards protects both buyers’ and sellers’ anonymity.

Packstation: New dropping means
German underground players have devised an interesting dropping means, one that involves fake deliveries. Most underground markets rely on droppers who cash in stolen credit cards and online accounts. There is no longer a need for droppers in the German underground. Users instead rely on the so-called “Packstation service” that takes advantage of the German postal service. This allows sellers to put goods sold in publicly accessible metal boxes for their buyers to pick up using their pTANs and access cards.

Figure 15: Banner ad for Packstation services
Somehow, German cybercriminals have taken advantage of an efficient system for fake deliveries. Packstations allowed for the convenient exchange of goods and payment. Users’ addresses cannot be tracked though they need to apply for the service using a physical (home) address and a mobile phone number (which are easy to fake) so they can receive short messaging service (SMS) notifications along with their pTANs to claim their parcels.
Figure 17: Post selling Packstation accounts with mobile phone numbers
Buy whatever you want (without spending anything) from online shops like Amazon or Zalando that allow Packstation delivery.

Get a bitcoin wallet. Contact the Packstation service provider and buy a hacked account. (Note that there are two types of Packstation accounts—one that is bound to a mobile number and email address and another that is “clear,” which means you can use a mobile number of your choice.)

**Figure 18: How cybercriminals avail of Packstation access**

**German-plaza.cc**

Pressure to ensure seamless and quick sales transactions brought about underground marketplaces that are replacing forums. Underground marketplaces are virtual shops of standardized goods—places for buyers and sellers to trade in a clearly regulated fashion. They have standardized procedures and can quickly process payments aided by technically enforced rules, making them more efficient for the exchange of goods and payment than forums. Though trading in forums is much slower, customized items (those that require modification and special pricing) are still exchanged more on them.

The German underground has several marketplaces for goods like drugs and credit cards. Among those we analyzed, german-plaza.cc stood out because it is the only actual marketplace where people can actually buy and sell goods (hacked accounts, traffic, etc.) and it is a purely German development.

Though not yet fully mature, german-plaza.cc has a wide variety of offerings. It has after all only started operating at the start of this year. We expect to see it quickly grow along with others of its kind. Prices are tailored to the German market and are driven by supply. Some product categories only have a handful of offerings. Compared with the Russian underground, it does not offer as many global products. The scarcity in offerings could partly be due to its beginner status. But it could also be due to geographical and language focus. German-plaza.cc, like the German underground, is a place for cybercriminal wannabes on the lookout for German-specific items like stolen Packstation accounts or German credit card credentials.
Figure 19: German-plaza.cc offers hacked accounts, stolen credit cards, data dumps (probably contain personally identifiable information [PII]), online game license keys, Packstation accounts, root access to servers, vouchers, and VPN services

German-plaza.cc’s Accounts tab features a wide variety of German-specific products. It also offers stolen online banking accounts most likely acquired via phishing. Cybercriminals can choose from an array of accounts according to bank type, balance, or price, depending on what they hope to use the goods for. Information on banks’ online processes and verification systems (using telephone personal identification numbers [PINs]), which cybercriminals may not be familiar with, are also given.

Figure 20: Online banking accounts sold in german-plaza.cc
Figure 21: Online banking account information available in german-plaza.cc
German-plaza.cc sells hacked online bank accounts for at least €10 (US$10.66), depending on their available balances and the amount of information (owner’s personal information and telephone PIN) tied to them. One account, for instance, costs €2,750 (US$2,932.33). This could be because of its high balance (€7,500–8,000 or US$7,997.25–8,530.40) and the fact that it comes with a telephone PIN and owner’s personal information. Knowing this information is crucial, especially since banks are alerted when huge sums of money are moved from one account to another. If that happens, the cybercriminals will need to provide the right information should they receive a phone call from the bank.

Figure 22: Details on an online banking account sold for €2,750 (US$2,932.33) on german-plaza.cc
Some online banking accounts also come with telephone support. This means that buyers will take care of all verification calls from banks.

![Figure 23: Ad for professional telephone support for bank verification calls on german-plaza.cc](image)

Credit cards and PII dumps are pretty standard items in underground marketplaces. German-plaza.cc offers credit card packages that include owners’ addresses, card expiration dates, and so on. Knowing this information is critical for those who wish to use stolen cards to make online purchases or clone cards for physical use (in actual stores and establishments).
Online game license keys and account information are also sold in german-plaza.cc. Users can also purchase Packstation access on the site. Stolen and fake vouchers for Amazon and similar online shops are also sold. These can be used to buy something on the real sites or as payment for goods bought. Vouchers are easy to phish and are quite in demand.

Root access to servers is obtained by buying credentials. These servers can be used to proxy Web traffic and set up sites to host malicious content. Prices are dependent on supply.
Malware made in Germany
Trojans, exploit kits, and other core crimeware can be seen in the German underground but these do not make the market unique. What we would like to focus more on are locally developed tools. It is interesting to note that some German cybercriminals develop Web applications for money. One coder, in particular, has been praised by many users for his skill and delivering what was promised.

![Figure 26: Banner ad for coding on demand](image-url)

![Figure 27: Praise for coding on demand who produced a fully functional phishing script with anti-blacklisting feature](image-url)
Sphinx, Cube, and Triple CCC

We also saw a few tools that were advertised first on German underground forums.

Sphinx and Cube

Though Sphinx and Cube can be found in Russian forums, they were first advertised in German forums, leading us to think they were developed by Germans or at least people who were active in the German underground.

Sphinx⁶, a ZeuS variant, is written in C++. Its authors designed it to operate in TOR, making it immune to sinkholing, blacklisting, or tracking.

![Sphinx Banking trojan]

**Figure 28:** Crimenetwork.biz ad for Sphinx
Figure 29: Sphinx’s configuration panel

Figure 30: Sphinx’s active bot statistics panel
Cube, meanwhile, is a tool that cybercriminals can use to recover files from infected machines that are part of a botnet. It has ties to the site, nodistribute.com, which anonymously scans malware against the most popular antivirus products.

![Cube’s control panel](image1.png)

**Figure 31:** Cube’s control panel

![Cube boasts of working on all of the platforms mentioned in its properties panel](image2.png)

**Figure 32:** Cube boasts of working on all of the platforms mentioned in its properties panel
Triple CCC

Triple CCC, a German product, has a malware and C&C component. It is basically a Trojan that steals passwords from infected machines. It infects machines when a link embedded in an email is clicked or via an exploit. It can steal passwords from a lot of software, along with browsers, messengers, and File Transfer Protocol (FTP) servers. It can also steal Microsoft™ Windows® license keys along with credentials to download managers. It is sold for 25 BTC in the German underground.

Figure 33: Ad for Cube Recovery 4.1 for €3 (US$3.20) worth of bitcoins on crimenetwork.biz
Figure 34: Platforms and software that Triple CCC can steal from

Figure 35: Triple CCC’s control panel
SECTION 3

German and Russian underground overlaps
German and Russian underground overlaps

German and Russian underground forums are littered with carding service banner ads. These are usual Russian underground offerings that are heavily advertised in German forums. Rescator.cm, one of Russia’s biggest stolen credit card marketplaces, and SecureVPN.to also figure in the German underground. We can assume that German cybercriminals often visit the Russian underground to learn from their big brothers. It is also safe to assume that collaboration between German and Russian underground market players happens.

Overlapping profiles

We came across one particular cybercriminal that sells wares on both the German and Russian underground markets. One of his primary offerings is Loki Bot, a well-known botnet framework sold on various forums. It was first sold in the Russian underground forum, “Damage Lab,” then made its way into the German underground’s crimenetwork.biz. Its owner is also a very active seller of stolen credentials in several Russian underground forums.

Figure 36: Ad for Loki Bot found in Russian underground forums
We have seen other users figure in both underground markets as well. We cross-checked several thousand nicknames obtained from German forums against those from Russian underground forums and saw overlaps. Around 300 users actively operated in both communities. This led us to believe that substantial collaboration between German and Russian cybercriminals occurs, an almost natural development because cybercrime knows no borders. Note though that our comparison was just based on the language the cybercriminals used. We did not compare the German user list with those from other markets (China, Brazil, Japan, and North America) because we believe the Russian underground is still the most seasoned to date.

**Shared resources and parallel sites**

We stumbled across a German site that sells stolen credit cards (centralshop.cn), which looked very similar to a carding site in the Russian underground (gocvv.cc). This prompted us to further investigate if they were connected to each other. As it turns out, they shared a database and application framework, which again suggests German-Russian underground collaboration.

![Figure 37: Centralshop.cn’s (left) and gocvv.cc’s (right) home pages](image)

![Figure 38: Gocvv.cc’s (Russia, left), centralshop.cn’s (Germany, middle), and 2force.cn’s (Russia, right) log-in screens](image)
Further research revealed that all three marketplaces—gocvv.cc, centralshop.cn, and 2force.cn—are partner sites. They use the same credit card database and graphical user interface (GUI) with slightly altered designs and content to fit their clients' needs (mostly dependent on the language used). Each site takes care of its own domain registration despite using the same database and GUI. Each site also takes care of its own promotions mostly via banner ads.

**Cross-market advertising**

Anonymous file sharing is common in German underground bulletin boards. It allows users to upload and share files (usually copyright protected) with others. Vanille.cc is an example of such a service that is heavily advertised on German underground forums. It is owned and maintained by a member of the Russian underground but heavily used in the German market. As such, it could be a product of German-Russian underground collaboration.

The German underground is a small but mature-enough ecosystem that caters to the basic needs of local cybercriminals. It has dynamic ties to other underground markets, particularly Russia's. We looked at the market’s general setup, components, and offerings. We specifically analyzed wares unique to the German underground like hacked Packstation accounts and marketplaces that catered to the customized needs of its local clientele.

We found that seasoned cybercriminals looked at offers in bigger markets like the Russian underground while those who are just starting out and need customized wares go to niche market's like the German underground. We specifically looked at german-plaza.cc and saw that it is a growing marketplace that is positioning itself as a trading ground for all sorts of crimeware. Though the German underground is still young, its malware coders are skilled, even offering coding services on demand.

In many ways, German and Russian cybercriminals collaborate with one another. We even determined quite a number of users who operate in both environments. This connection was made even more visible by partner sites that not only look like each other but also offer the same wares (using the same database) even if they use different domains. This isn’t surprising though given the borderless nature of the cybercriminal underground.
Appendix

User Guide for “Packstation”**

Step 1: Bitcoins

Bitcoins are ubiquitous in the scene and have taken the place as an anonymous means of payment after the bust of Liberty Reserve.

Bitcoins can be purchased in different ways, I recommend Virwox.com. There you can easily buy bitcoins via direct transaction, credit card, PayPal, Paysafecard, Ukash Skrill (Moneybookers), and Neteller.

Since you still require a wallet before you can send/receive bitcoins you should definitely register on Blockchain.info Register, where you can receive/send bitcoins—it’s a very reliable service!

Depositing at VirWoX!

Once you have deposited money, it will show on your account balance, and you can acquire bitcoins. For that go first to EUR/SLL to purchase Second Life currency, then you can convert the currency into bitcoin under the category BTC/SLL.

Now you can cash out your bitcoin; for that create a new address in your Blockchain.info Wallet, select “cash out” at Virwox.com and include that address and the number of bitcoins that you want to send. The first deposit Virwox.com will take 48 hours since the payment will be checked manually in order to uncover fraud, all further payments will then be transferred instantly (at least with me).

Step 2: Sellers of Packstation accounts, Gold cards, and credit cards

Rippers are everywhere, ripping in the scene has become a new business model—whether it’s €5 or €15 it doesn’t matter, the main thing is money without any service in return!

I offer you a small list of retailers, very thrustworthy sellers!

Packstation

Ohman on crimenetwork.biz

Packstation without number and with email access—€20 (€15 if action takes place—bulk discount)

Packstation with number and email access—€2 (minimum purchase of 10)

ICQ Number: XXXXX

** The contents of this section have been loosely translated from the original text in German.
Gold card

Wax on crimenetwork.biz

Wax is one of the few Gold card sellers, whose Gold cards also are really gold, not white blanks!

Gold card—€7 bitcoin, with TID €3 surcharge

If you buy a Packstation with Ohman, you can receive the Gold card at Wax.de for €5 instead of €7.

Credit cards

I have seen a lot of CC-sellers come and go, the quality really varies and often you get quantity instead of quality for the price BUT there is one person/shop that really stands out because he offers really good quality

Razzia.biz

Classic random €4

High-Limit random €8

Classic fullz €30

High-Limit fullz €50

It’s not one of those disgusting sahnescript shops where you have to contact “Live Support” just to cash-in bitcoin; Razzia.biz really gets you your good instantly.

You select your products, add your ICQ number to (you receive the product via ICQ but also locally on the site) do the captcha and buy it. Then a window with a bitcoin wallet and the number of bitcoins appears; transfer it via Blockchain.info and select “Paid” with Razzia.biz, then the script checks if your bitcoins have arrived—two confirmations are required!

Step 3: What is the difference between Packstation packages?

Packstation with number and email access—a cost of ~€5.

Here within the panel of DHL a cell phone number has already been saved, this number is important for the mTAN (similar to online banking)—the mTAN is required in order to to pick up the package from the Packstation.

It is possible to change that telephone number via support using SE (social engineering), loss of cell phone’s, a new contract mobile phone with a number etc.
Packstation WITHOUT number and email access—a cost of ~€20–25.

Here you can simply enter the number of your anonymous SIM card (Anosims.biz offers these)‐quickly before dropping—and so you can drop your packages without having to be in contact with DHL employees.

Step 4: Ordering—Which other shops offer delivery?
There is a plethora of stores that deliver to Packstations, ideally one should not directly opt for the large providers such as Media Markt, Saturn, or the like.

For example Zalando delivers to Packstations, just like some smaller stores.

The best course of action is to opt for shops that nobody knows well, obviously it is not easy to find such shops but from time to time you will find some just with a little help from Google.

Hall of fame: Active underground forum usernames

The following nicknames were used by active German-speaking forum users featured in this research paper.

Secunet.cc

allinkl Allremerbers Alt4r Ambutaga aminekojim AmmarShaarawi anomaly ArNd Andrej annax8 Anonymous anx112 Ansgard Ar3a aoddac ASPF0815 ashmax Auros avanrin Br j.x x bkerstll b0st1337 B1nary B2H B3ND3R B3ND3RZ b3nua B3RBY B4nQoe737 B4sI babal backpackhacker bananabob barreta bbbing ben berlin2I BewI bezen Bierdeckel B1son BLlCode Bitschi b0Wf1sh big4f backbez BlackDesert BlackEagle BlackHook bladeronion Bloodman BlueEyes boing727 bommel BomB Bom2hacK BossGen Brabus12 Brokole BuntspechT bursali cd03x cJph3r C1T c3bob Caudex Cent0x CEOmADDIN ch3m chabarnaba CheEtAlH chick0n Chystal c91091 comic conrado cooky1 CoolFroG Corono cR3v61 Cr4ck3r crlmetology CTU Cube Curuba CyberTjak CyberEnte CyberSpy D0b d2muX da_vinci dagunn DarkSmile Darkhammer dasemih dasedz dbmnm dec0 Dedhore deluxeBro Dennar derhaxxxxxxxxxxxxxxxxxx0 DerAuslnder dermildeinBuch DerWilliGottes DeSSo devilink Digitaltourist Domenic double_check D0x drbob DrFalkenhorst DrSecurity DF.Lyztz Drohne Dysystem Dynamoking easy easyamigo Echo88 ef.Jay elo317 EinstiegsGamer Eiswürfel ELIT3 ELIT3 EliteSoldier Eliteterror Elvis enmi EnnmJack EmcoCore1990 EmX EssHaa exo2 Extasy ExtasyB Eye ezah FOX Fat11 Failer FallOut Fapter feler FIM4LSHare firecrash fish3r Fl00der Fl0ckz Flame0 flashbang Fischpeitsche flownn Found57 Fox FR3DDY Framerater Freudefeindlich frechdax Fred_durst Frost Fruity g-suz gatIgt gehaxter GeizerDarkICE Genet1C GhostPlug ghosty golan Gothberg GP120 Graf dtx Grax groks gutzuu H0RR0R H4CK00R H4CK3R hlx0r habanero hackhol hackolli hacktainer Hades HaeckerUpdate habegnarry HAK Haksox Halux HansPeter Harry Haupling Hawek hbDEhuusV HCPHLS He4dPhron3z Hedrek HikaKin Hoax-TX Heli holomaster horstwald hugo12 hur_durr i3c Ice icemans idontfeelanything iDope illusI0n ImNichts IMPEGA Imperial INCEPTION Installous InternetFreak iPen isabella09 J_Bunny Jbnn X3r j박bukk jebiga30 Jerycan JigSaw JLine joeroot Johannes JoyIyna Jonas JPK Juleh junkfood justnew k3r k3uL3 Kain101

42 | U-Markt: Peering into the German Cybercriminal Underground
The text in the image contains a list of usernames or handles, likely related to cybersecurity or hacker communities. The text is long and contains many individual entries, each representing a different username or handle. The usernames are diverse and include abbreviations, numbers, and various combinations of letters, possibly indicating different levels of access or roles within a cybercriminal or hacking forum.
References


