The French Underground

Under a Shroud of Extreme Caution

Cedric Pernet
Trend Micro Cybersafety Solutions Team

A **TrendLabs**SM Research Paper

Contents

If the North American underground had an alter ego, it would be the French underground. A deep dive into the North American underground[1] revealed that it is a "glass tank," open to not only the tech-savviest of hackers, but also visible to both cybercriminals and law enforcement. The French underground, meanwhile, is not only well-hidden in the Dark Web, its players also operate with extreme caution.

An air of distrust surrounds the French underground, much like the Japanese underground[2]. Japanese bulletin board systems (BBSs) used CAPTCHAs to filter users, making sure they were Japanese nationals or at least speakers. The French took this up a notch, as their underground forums, marketplaces, and autoshops (a unique business model) either required membership or some form of vetting prior to participation. Forum administrators only allowed people to become real active members after obtaining a certain reputation score. Some forums also ranked users in terms of experience. They treated newbies differently from more experienced cybercriminals who have, in essence, gained "elite," "administrator," or "trustworthy" status.

Escrows were a must in business transactions in the French underground, as in its Russian[3] and German[4] counterparts. They made sure that buyers and sellers got their due end of the bargain. Unlike in the Russian and German underground markets, however, shaming ran rampant in the French underground. Every forum had a "hall of shame" or means for reporting dishonesty or fraud. Forum owners and/or members often shamed their rivals, discouraging others from patronizing the latter's offerings. Marketplaces also often went to war against one another in an attempt to get more members or even the money of their rivals' members, aided by the fact that French cybercriminals were often members of more than one marketplace.

Unlike the bigger and more established markets—Russian and Chinese[5]—the French underground is still quite small, only made up of around 40,000 cybercriminals (ranging from common thieves to masterminds) amassing €5–10 million per month based on the Gendarmerie Nationale and Police Nationale's estimates. It can be likened more to the German underground, which has niche offerings. French cybercriminals relied on bigger markets for most of their needs (malware, other tools, and services). Much of the underground market's offerings can only be used in committing fraud against the French-speaking public. These include mailbox master keys and fake receipts/bills, and bank-account-opening services, among others. Mailbox master keys can be used to steal personal documents that can be used for committing identity fraud. Fake receipts/bills, meanwhile, can damage the reputation of retailers/companies being defrauded. Finally, bank-account-opening services, aided by credit card credential theft, allow criminals to commit bank fraud. But that doesn't mean cybercriminals can find staples in the French underground. French cybercriminals do dabble in creating their own tools. Of particular interest are locally produced ransomware[6]—probably the biggest security threat to date. They also offer data dumps (stolen user credentials) and tools like binders that aid in attacks to individuals and businesses alike.

Overall, the French underground is a small market that caters more to niche requirements for committing fraud against the French-speaking victim base. It operates under a shroud of caution. Its players are not only wary of law enforcement agencies that implement stringent cybercrime laws, but even of players (forum/marketplace/autoshop administrators/members) who may be working with the former. Amid such seemingly blinding lights shining on it, is the French underground bound to thrive like its big brothers? And if it does, what can the security industry do about it?

SECTION 1

The Anatomy of the French Underground

The Anatomy of the French Underground

What is the French cybercriminal underground like? How is it structured? How does the French culture figure into it? These are just some of the questions that we will answer in this section. We hope to shed light on what sets the French cybercriminal underground from the rest of its counterparts spread around the globe.

Wary and Cautious amid the Blinding Lights

Like any bad guy, a French cybercriminal handles business with a single thought at the back of his mind—he must evade law enforcement. But probably unlike criminals in other countries, those in the French underground are more cautious. They're stauncher believers in the adage "no honor among thieves." This is reflected by the fact that every forum has a feature for reporting dishonesty or fraud—a "hall of shame," if you will. The atmosphere of distrust doesn't stop there though. Apart from a hall of shame on every forum, owners and/or members often shamed their rivals, discouraging others from patronizing the latter's offerings. Marketplaces often went to war against one another in an attempt to get more members or even the money of their rivals' members. Cybercriminals were often members of more than one marketplace. In a recent example, members of two marketplaces—A and B—were caught in the crossfire. Marketplace A's checked who among its members were also members of marketplace B. The administrators then stole and tried to use the members' marketplace A credentials to hack their marketplace B accounts. This allowed the administrators to steal all of the Bitcoins that were tied to the member accounts that they hacked if their owners used the same credentials for both marketplaces. Fortunately, the rival marketplace's administrators were usually quick enough to cancel unwarranted Bitcoin (BTC) transactions, probably because they have been warned by hacking victims.

In the course of doing research, we found a major forum that suddenly disappeared, which turned out to be a normal occurrence in the French underground. Forums and marketplaces constantly emerge and

vanish, again most likely due to the overwhelming fear of law enforcement and fights among marketplaces. French cybercriminals always worry that law enforcement agents in the guise of either sellers or buyers are always watching their every move. To address this, forums relied on vetting systems. Forum administrators only allowed people to become active members after obtaining a certain reputation score. A person's reputation score increases with every incriminating post or successful fraudulent transaction made on the forum. In essence, the higher your reputation score is, the more trustworthy you are (which translates to, you're not a law enforcement agent). Apart from using reputation scores, some forums also ranked users in terms of experience. They treated newbies differently from more experienced cybercriminals who have, in essence, gained "elite," "administrator," or "trustworthy" status.

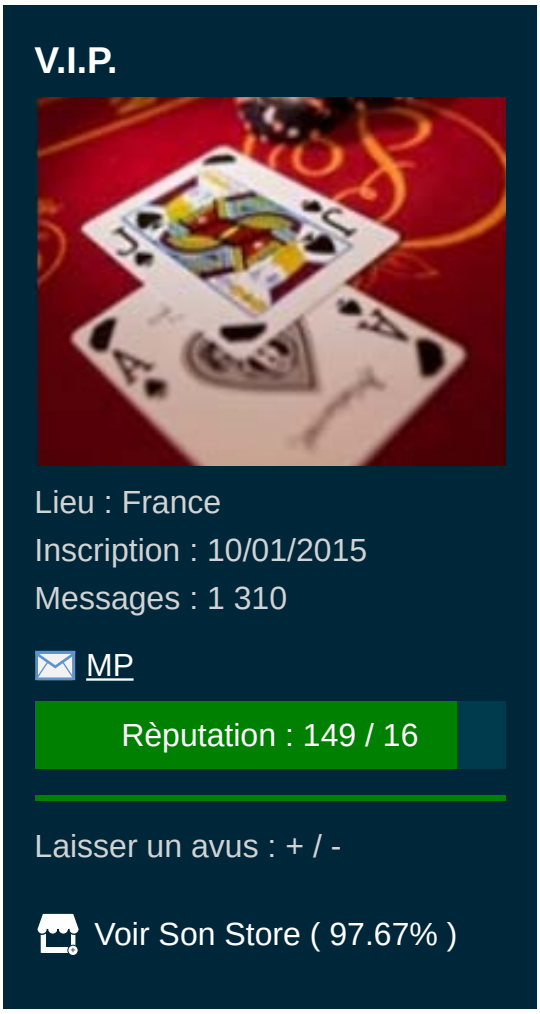

Figure 1: A user's reputation in a marketplace is displayed on his profile

This overall sense of paranoia could also be the main reason why cybercriminals encrypted their communication. All of the forums we found offered the possibility to encrypt even the messages sent over their own private messaging systems. Even message board administrators could be suspected of reading members' private messages. This could be due to a past incident when a member of the cybercriminal underground community leaked private messages from several forums to law enforcement officials.[7]

The French underground is rife with distrust that like the Russian and German markets, escrows abound in it. Escrows are third parties that act as middlemen in two-party transactions. Escrows make sure that buyers get what they paid for and that sellers get their money for a fee, of course. They typically get 7% of the total transaction amount if it's less than €500 or 5% for total amounts over €500. Unlike Russian and German marketplaces though, escrows are limited to a total transaction amount of €1,000 in some French marketplaces. Every time they reach this amount, they have to wait until all transactions are processed before they can engage in others.

Escrows are so commonplace in the French underground that Intelligence Black Market (IBM) had its own semiautomatic system. Each escrow got 4% of the amount of every transaction. The system known as "Autoescrow Platform" is independently hosted, allowing it to run even if the forum is undergoing maintenance or suffering from connection problems. It even has two-factor authentication (2FA) features for enhanced security.

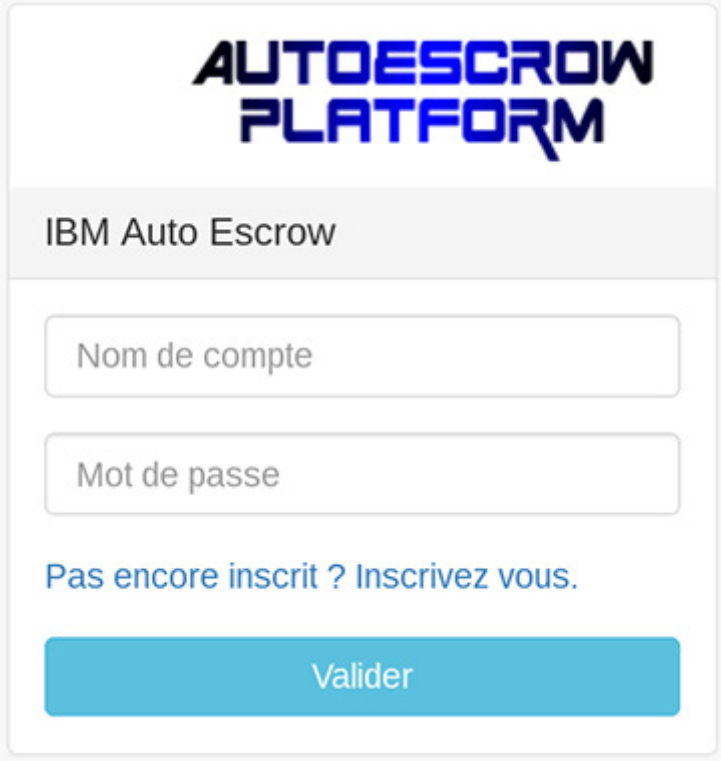

Figure 2: IBM's Autoescrow Platform log-in prompt

If the North American underground is a "glass tank," open to not only the tech-savviest of hackers, but also open and visible to both cybercriminals and law enforcement; the French underground is its complete opposite. Much like the German underground, the French market entirely resides in the deep recesses of the Internet—in the Dark Web.

How Do Marketplaces and Autoshops Differ?

There are roughly three ways for fraudsters to sell illicit goods and services in the French underground. Some simply advertise their wares in popular marketplaces. Others prefer to stay well under the radar, not advertising but profiling potential buyers then more directly approaching them. But probably most common and, arguably unique to France, is by running so-called "autoshops," small online shopping places owned and operated by the sellers themselves.

Forums can have their own marketplaces. But while others are easy to find with a single search engine query, most are well-hidden. French cybercriminal marketplaces don't differ much from those seen in Russia, China, and Brazil[8]. They offer all sorts of crimeware at very competitive prices. Their only unique feature perhaps is the fact that they sometimes require membership fees and vetting.

In a way, the French and Japanese underground markets are less trusting than their other country counterparts. Their forums (bulletin board systems [BBSs] in Japan) both require some form of authentication prior to obtaining access.

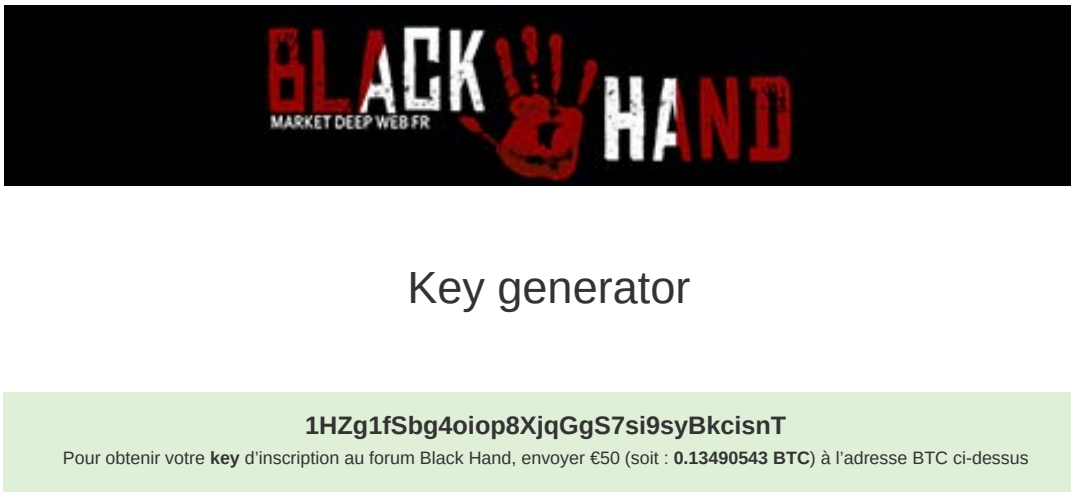

Figure 3: A French underground marketplace that requires a €50 (in BTC) membership fee

More commonly seen, however, are autoshops that advertise on various marketplaces and forums. Each autoshop is owned and maintained by an individual. This individual directly deals with potential customers and buyers. The exchange of illegal goods and services is more direct.

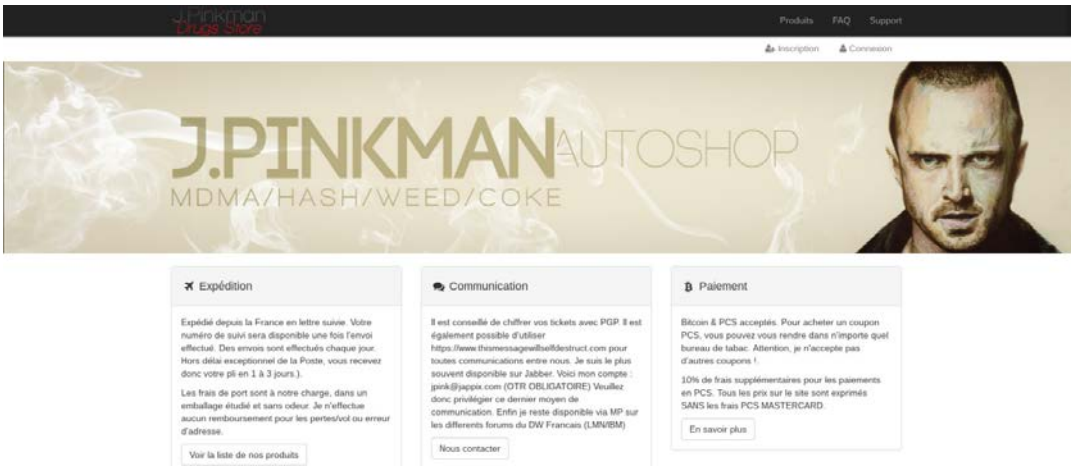

Figure 4: A French underground autoshop that sells drugs

Autoshops are so popular in the French underground that some cybercriminals earn a living by providing autoshop-creation services. For €400, they can give you your own Dark/Surface-Web-hosted autoshop, complete with Content Management System (CMS), within a couple of hours. They take care of everything, including domain registration, installation and hosting, customization, and even backup.

Figure 5: Sample autoshop CMS that comes with autoshop-creation services

Bitcoins and Prepaid Card Services: French Criminals' Preferred Payment Means

Trust issues—both in law enforcement and their peers—could be the primary reason why French cybercriminals only accept two forms of payment—Bitcoins and Prepaid Card Services (PCS).

Using Bitcoins provides a certain level of anonymity to users. They are easy to obtain and transfer without need for proper identification, as the currency remains deregulated.

PCS cards, which are prepaid payment cards that can be bought practically anywhere in France (even online), have become popular among shoppers, illicit or otherwise. Some merchants don't even require buyers to provide proper means of identification (ID) when purchasing and reloading PCS cards. All they need are working mobile phone numbers, which are easy to obtain. This, unfortunately, makes them ideal payment means for illegal goods and services.

PCS cards have become so popular that some cybercriminals sell PCS cards, along with scanned copies of fake owners' national IDs and personal information (home address, email address, and a subscriber identity module [SIM] card which was used to register the PCS card) to peers. The buyers then use the fake PCS cards to receive payment for the illicit products and/or services they sell to their own customers.

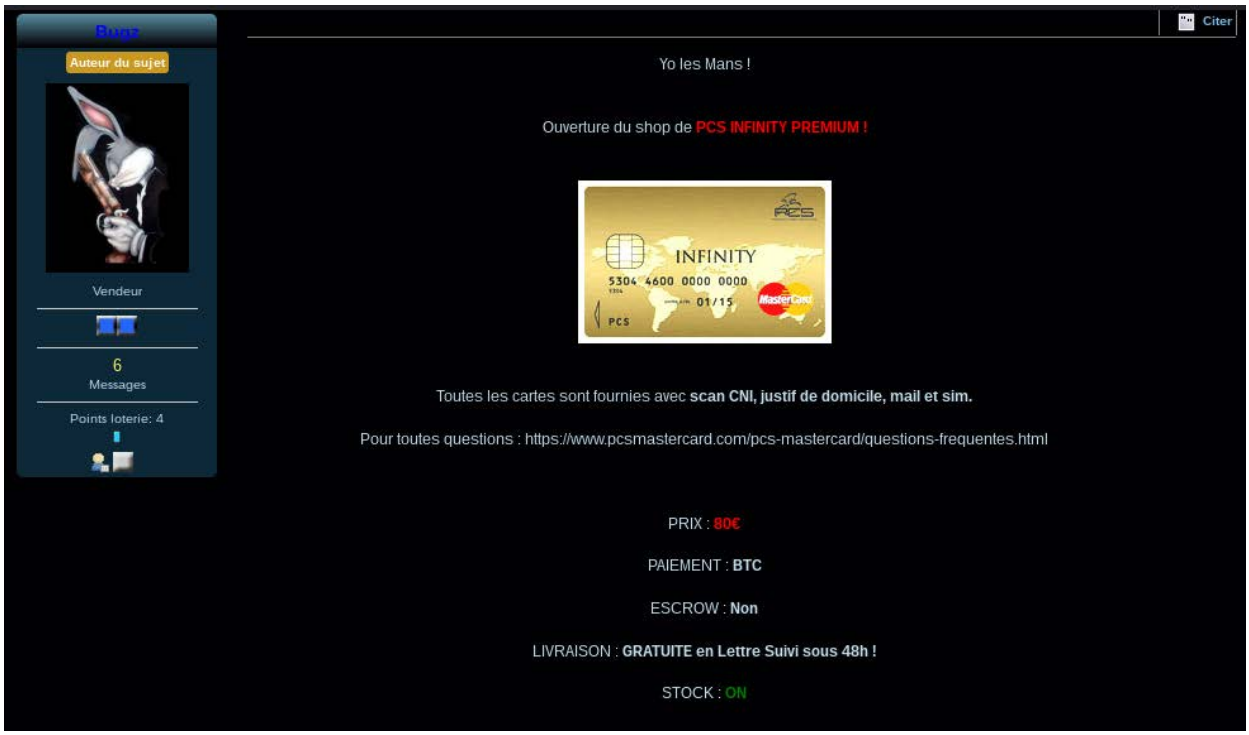

Figure 6: Ad selling a PCS card complete with the fake owner information for €80

SECTION 2

French Underground Offerings

French Underground Offerings

The French underground is a mixed bag of offerings, like any other cybercriminal market. It has goods and services that are uniquely French and those considered staple crimeware. Note, however, that our research mostly focused on the five biggest marketplaces in the French underground, along with two forums, which were not exactly tied to specific marketplaces.

Uniquely French

"Secret" Weapons

Every cybercriminal underground market has its own section for weapons for sale. Unlike most markets though, the French underground caters more to buyers of "secret" (small and inconspicuous) weapons instead of big, powerful guns.

Figure 7: "Pen gun" sold in a French underground marketplace for €150

Secret weapons, including brass knuckles and small knives, cost very little, around €10 each. They are usually camouflaged or made to look like harmless objects. You can, for instance, find flexible knives shaped like credit cards (€10) and pen guns that shoot .22-caliber Long Rifle (LR) bullets (€150) because it is absolutely forbidden to carry any kind of weapon in France.

That doesn't mean heavy weapons aren't available in the French underground. They just cost a lot, often sold for hundreds to thousands of euros (€650–1,800), again probably because owning such weapons is forbidden in France.

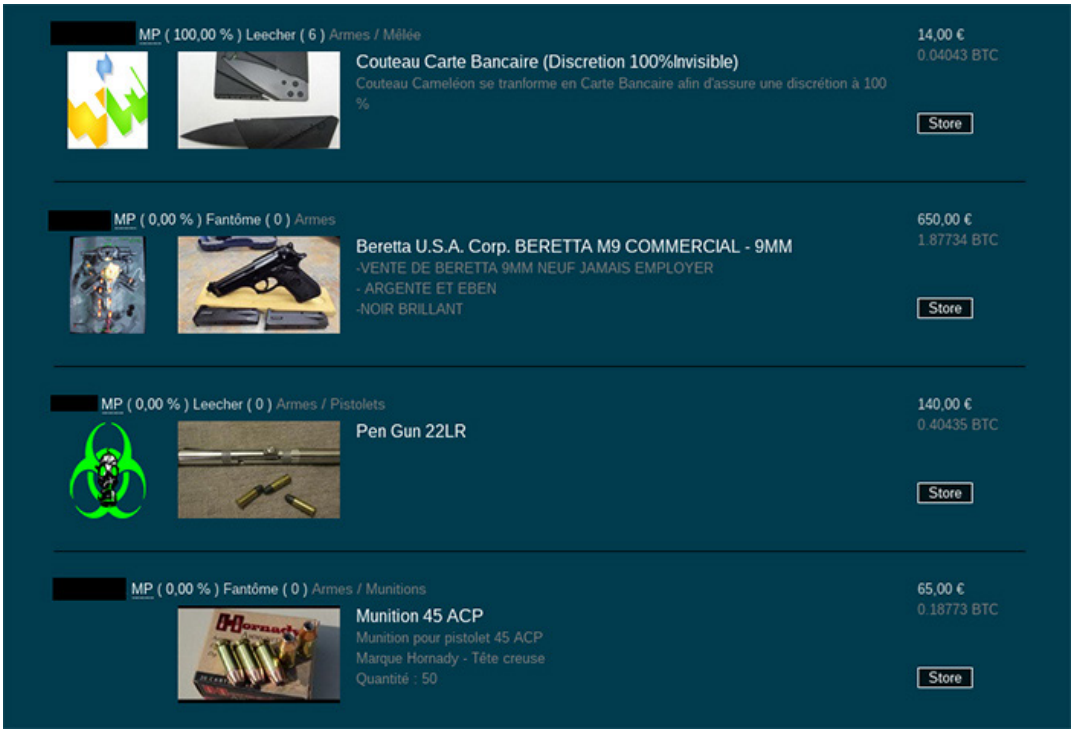

Figure 8: Variety of guns sold in the French underground

More interesting, however, are file packs for 3D-printed guns. A file pack sold for €4 each can print 12 different guns, including AK-47, Glock 17/22, and MAC-10. This is disturbingly affordable, not to mention that the pack doesn't come with an instruction manual for assembling the 3D-printed gun parts.

Suicide/Euthanasia Kits

Even more disturbing was a forum where a seller posted "KIT DU SUICIDE MEUTRE ou EUTHANASIE 100% de reussite," which translates to "Suicide Murder or Euthanasia kit 100% success." He wanted to know if there was a market for such a product because he didn't want to produce the kits if no one would buy them. He offered two different kits—injectable or drug—for €500 if the buyer uses it himself. If the buyer wants to use the kit on someone else, he'll have to pay double. This particular seller didn't get any buyers though, at least not publicly.

In a database dump of another marketplace forum, we found a thread between the same suicide/euthanasia kit seller and a buyer. The buyer wanted to buy a kit for use on someone else (in an obvious murder attempt). They bargained back and forth until they settled for a price of €600 paid in BTC.

Mailbox Master Keys

Some French delivery service providers such as La Poste own master keys that can open customers' mailboxes as part of their service. What their customers don't know though is that these master keys are readily available in various underground forums at very affordable prices.

We found a vendor selling 25 such master keys (a complete set) for €220. Others sell keys per piece at €15; still others sell three keys for €35 or 12 for €115.

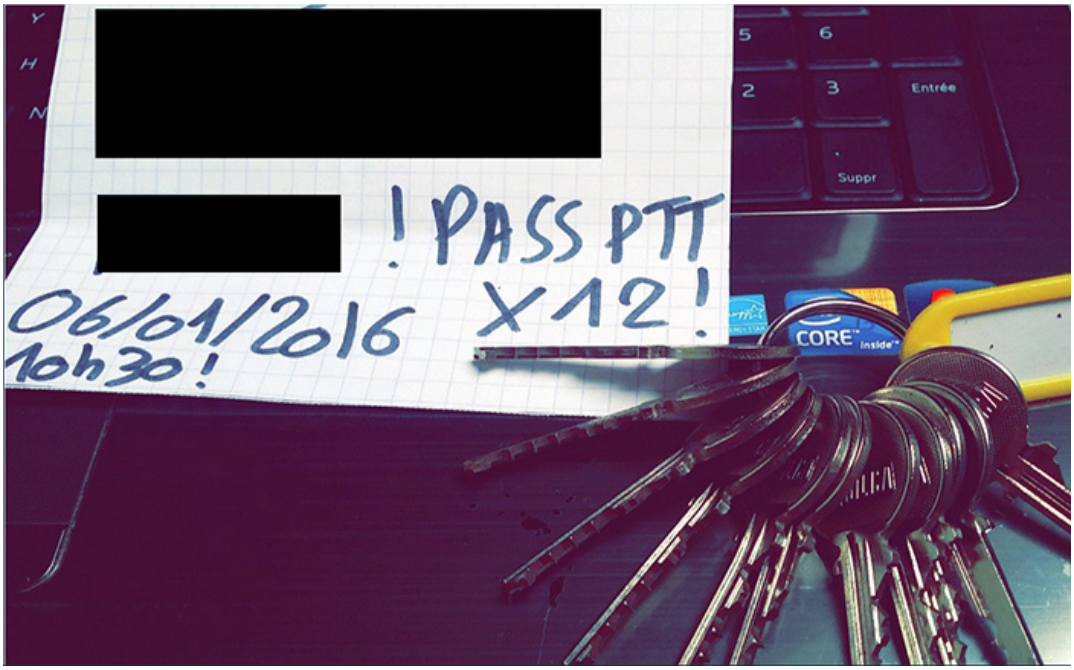

Figure 9: Set of 12 master keys sold underground for €115

While almost all mailboxes in France can be opened with only four master keys, other keys can also be bought to open mailboxes in remoter areas of the country. Some also open doors or other locks (not just mailboxes) in certain cities like public transport passage doors and private entrances to buildings, among others.

Master keys are so popular that some scrupulous individuals even offer 3D-printing files of such free of charge. Not only do these allow cybercriminals to burgle other people's mailboxes for parcels and packages whose contents can easily be fenced, but also get their hands on private mail or government papers for committing fraud.

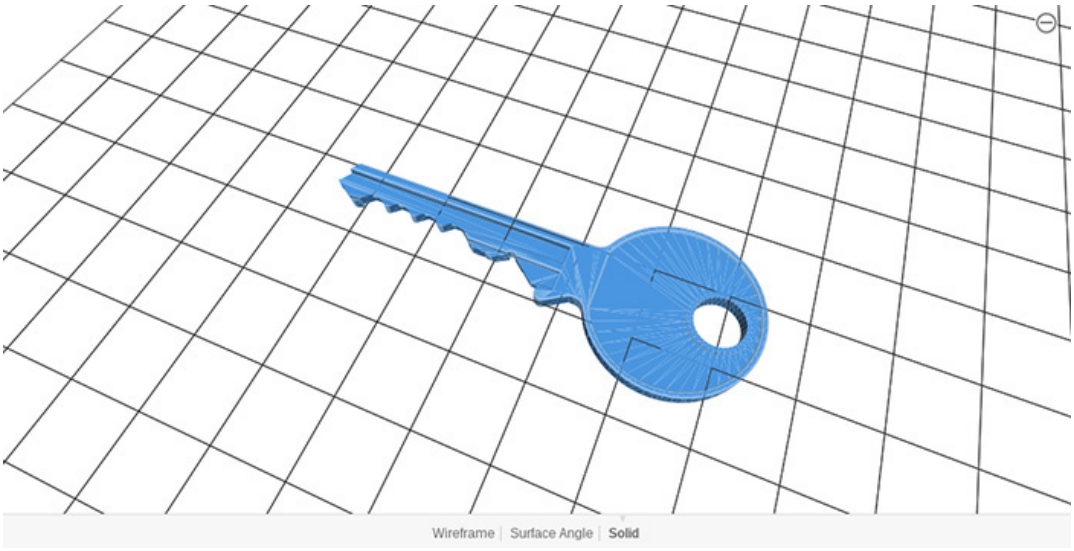

Figure 10: A 3D printer file of a mailbox master key offered free of charge

Fake Bills, Receipts, Car Registrations, and Checks

Fake bills, receipts, and car registrations are also sold in the French underground. Like other fake documents seen in most cybercriminal markets, these are made to look as authentic as possible.

Page 1 / 1

DARTY GRAND EST
Service Comptabilité
TSA n°80 004
93145 - Bondy cedex
Téléphone : 01 48 02 34 35
Télécopie : 01 48 02 77 80
0 978 970 970 (prix d'un appel local)

Livraison

Facturation

FACTURE
N°6159424 du 10/12/2013

Votre commande 989 040 0367863 du 07/12/2013

Référence	Qté	Libellé	Total HT	Base / Taux TVA ou TCA	Total TTC
1351036	1	Enceinte PC HERCULES XPS 101	133,77 €	26,22 € 19,60 %	159,99 €
		Dont éco-participation DEEE	0,84 €		1,00 €
		Frais de livraison			9,90 €

Le livret de confiance précise les garanties et services dont vous bénéficiez.

Total facturé :	142,05 €	27,84 €	169,89 €
Dont éco-participation DEEE :	0,84 €		1,00 €

Montant réglé par : Carte Bleue 169,89 €

Solde à régler : 0,00 €

DARTY GRAND EST - SNC au capital de 394 205 EUR - RCS LYON B 303 376 586 - code NAF 524 L
Adresse : RN6 - BP38 - 69578 LIMONEST cedex
TVA intracommunautaire : FR 13 303 376 586

Figure 11: A fake bill for Hercules XPS 101 speakers

Famous retailers in France like Amazon, Pixmania, and Darty, to name a few, are commonly spoofed for fake bills, which are commonly used in sale fraud. In this kind of scam, buyers are tricked into paying more for items without the retailer's knowledge. Extra proceeds then line the fraudsters' pockets. Others use the fake bills/receipts to feign the legitimacy of the stolen items they're selling.

Fake car registrations are also sold in the French underground. These allowed buyers to sell stolen cars at very low prices. By the time the buyer realizes that the car he bought was stolen, most probably when the application for new registration is flagged by the French Administration, the seller can no longer be found.

Figure 12: Fake car registration document sold at €500

Fake checks, meanwhile, are used to pay for any product sold in physical retail shops. Because there's no such thing as a fake check detector, some buyers get away with using fake checks with matching national IDs for buying products or paying for services rendered. Before banks detect the fraud, the fake check users can no longer be found. Fake checks are sold at an average price of €70–100 for 10 checks.

Bank-Account-Opening Services

Opening a bank account in France requires the applicant to present a national ID, proof of billing address and income, and other documents. And these documents aren't really part of cybercriminals' business dossiers. Bank account applicants are also required to make a personal appearance, which doesn't bode well for cybercriminals who don't want unnecessary attention. As such, French cybercriminals normally stick to scams that don't require wire transfers and other bank services to pull off.

French cybercriminals with bigger ambitions that require transferring huge sums of stolen money from a victim's bank account to theirs, however, can hire peers to open bank accounts for them. But because this entails taking a huge risk on the service provider's part, the service is quite expensive, often costing around €700.

Figure 13: Ad offering services to open French bank accounts for €700

Those who don't have €700 to spend on bank-account-opening services can opt to go it alone by purchasing and using tutorials that cost a little less, €400–500.

Driver's License Points

French driver's license holders have to abide by a penalty system if they want to keep driving in the country. A probationary driver's license holder gets six points; normal holders get 12. Each time they commit a violation, points get deducted from their license, depending on how grave their offense is.[9]

France's roads are all equipped with cameras and speed detectors that monitor all vehicles for speeding and all kinds of violations. But because cameras usually focus on plate numbers taken from behind cars, it's hard for traffic enforcers to identify who the drivers are. As such, it's possible to have points deducted from someone else's license if this is the one provided when a violator receives a letter from the state asking him to fill up the required form in order to settle a violation fine.

That's probably why we saw cybercriminals asking if anyone would be interested in purchasing driver's license points specifically for use within France's borders.

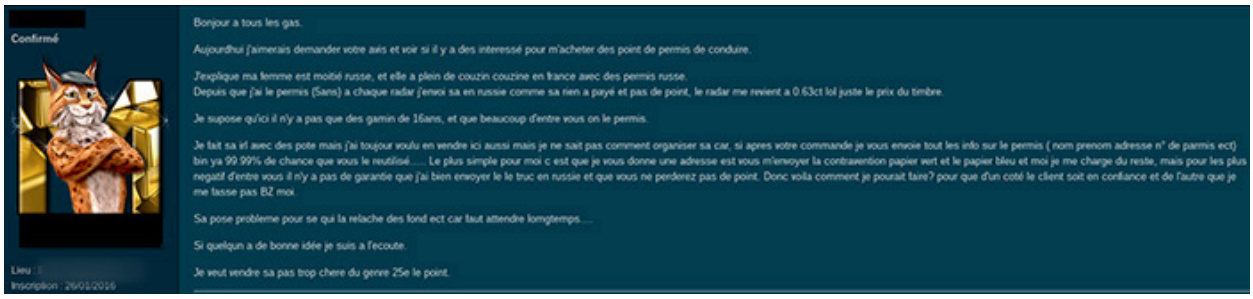

Figure 14: A marketplace member's post asking if it's worth selling French driver's license points

Cybercriminal Underground Staples

Ransomware

Ransomware are on their way to becoming the biggest security threat to date, if they aren't already. That's why it's not surprising to see that they are being sold even in a market as niche as the French underground.

We saw two cybercriminals selling ransomware. These seemed to be specifically intended for French victims. One was in the final stages of developing his creation, as he posted a screenshot showing how his product worked. It asked victims to pay in the form of BTC or via PCS or Paysafe cards.

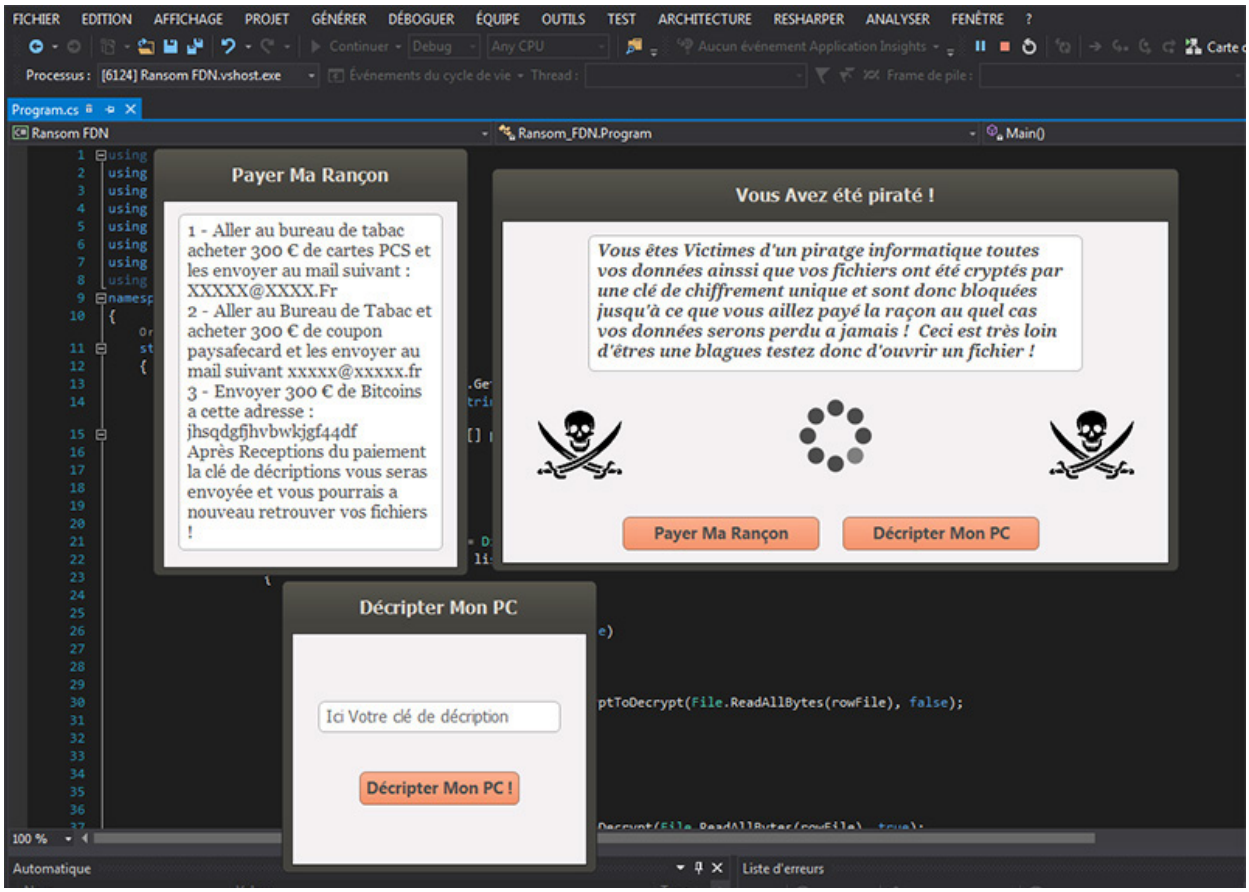

Figure 15: Screenshot showing the ongoing development of a French ransomware variant

The second ransomware variant, priced at €100, asked for payment in BTC.

Figure 16: The second ransomware variant's builder

Figure 17: The second ransomware variant's ransom note

Remote Access Tools/Trojans and Other Malware

As far as we can tell, most French cybercriminals purchase remote access tools/Trojans (RATs) and other malware from English-speaking underground markets. The only RAT still in use today, which was made in France, is Dark Comet by Jean-Pierre Lesueur[10], also known as "DarkCoderSc." DarkComet was developed between 2008 and 2012, before DarkCoderSc decided to stop developing it when it was used in a Syrian-conflict-related attack. It is, however, still available online and being used by cybercriminals even if it is already detected by any security solution when not heavily obfuscated, packed, or encrypted.

We did see an ongoing RAT project on a forum though its development seems very slow and leading nowhere.

Binders

French cybercriminals normally used crimeware (malware and tools) purchased from other underground markets to carry out their own operations. A few, however, still opt to create and sell their own tools that cater to requirements unique to the French underground. We found one such tool, a binder (a tool that obfuscates malware by mixing its code with legitimate software so it won't be detected by antimalware solutions), which isn't advertised or sold in any forum or marketplace.

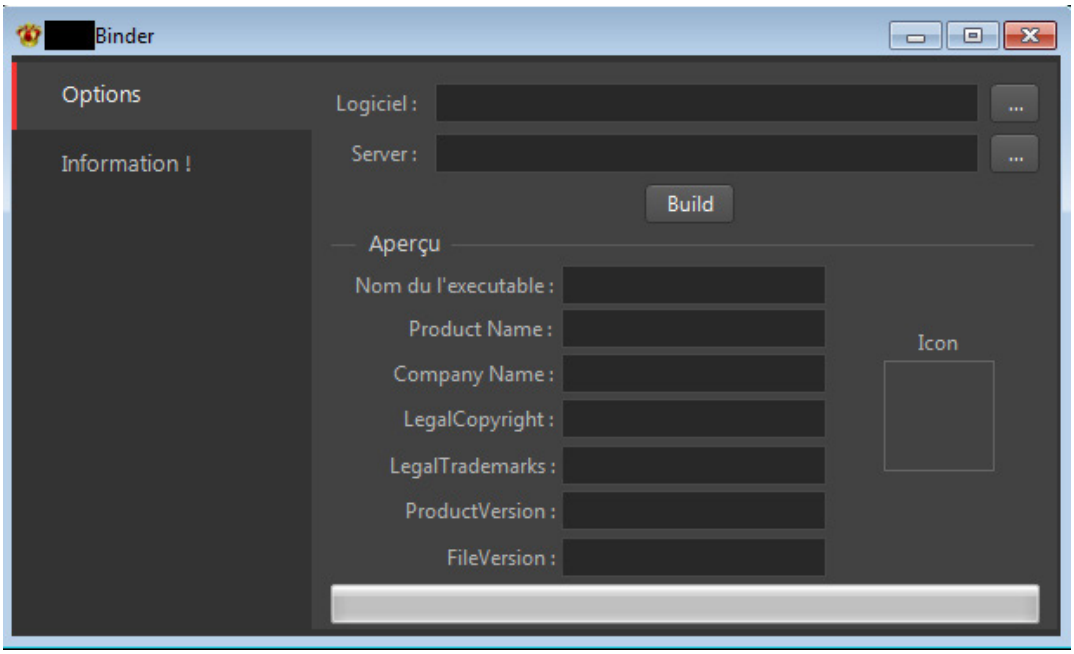

Figure 18: Binder created and maintained by a popular French malware developer that isn't advertised or sold anywhere

This tool proved particularly interesting because its developer (based on his name found in the user interface [UI]'s information section) is French. The UI also contained a message for two of the developer's friends who happen to be French malware creators as well. We believe these three malware developers use the said tool, along with a few chosen individuals.

Drugs

As in the North American cybercriminal market, drugs are also sold in abundance in the French underground. Cannabis or hash, depending on the quality and variant, usually cost €6–15 per gram. Cocaine; heroin; 3,4-methylenedioxy-methamphetamine (MDMA)/XTC or ecstacy; lysergic acid diethylamide (LSD); and mushrooms are also sold. Drug peddlers, however, only sell to customers within the country, a likely precaution to evade detection when crossing borders.

Figure 19: Ad for cocaine sold underground

Compared with forums in other countries, new drugs like bath salts or research chemicals/new psychoactives substances (RCs/NPSs) are not available in the French underground at the time this paper was written.

Other Crimeware and Illicit Services

Underground staples such as stolen credit card credentials and personally identifiable information (PII), along with proofs of identification, can also be bought in autoshops. Full database dumps can cost around €400.

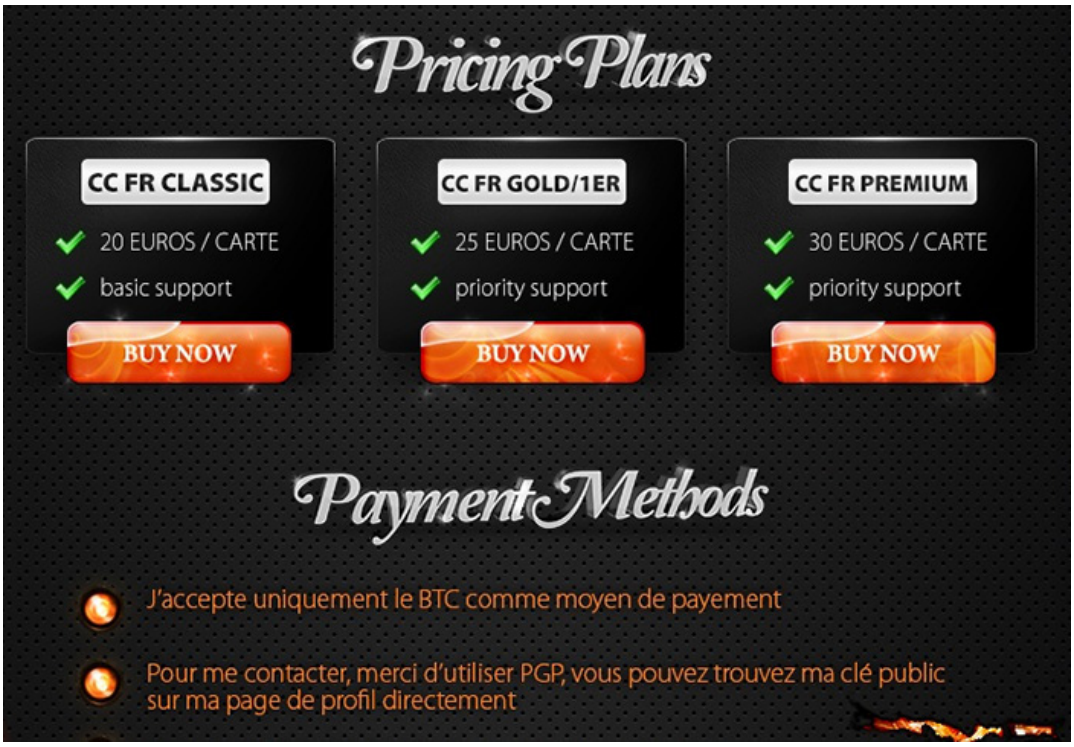

Figure 20: Ad for stolen credit card information

Figure 21: Auto'Scan v3 (an autoshop) ad selling high-quality scanned copies of fake national ID cards

The following table shows the crimeware and illicit services that can also be bought in the French underground.

Product/Service	Price
Fully undetectable (FUD) crypting service	€4–100
Bulletproof-hosting service	€10
Phishing kit	€100–500
Phishing page	€5
Phishing-website-creation service	€299
Botnet rental (100–150 bots/day)	€95
Fake national ID card	€60
Fake disabled ID card	€40
Fake document pack (ID and proof of identity)	€50–100
Teslin paper (used to create national/government ID cards; 200 sheets)	€167
Portable Document Format (PDF) file-editing service (including metadata modification)	€8
Fake money (€300 in €20 bills)	€135–150
Fake checks made out to specific recipients (10 pieces)	€70–100
Vulnerable website log (100 sites vulnerable to SQL injection attacks)	€30
Access to vulnerable website	€1–2
Software-vulnerability-scanning service (via source code analysis)	€219
Stolen credit card credentials (depending on limit/available balance)	€9–23
Automated teller machine (ATM) skimmer	€800
Credit card clone (depending on limit)	€40–110
Access to compromised PayPal account	€5–10
Access to compromised Amazon account	€10

Product/Service	Price
Fake shop gift card	50% of the card's amount
Access to compromised Facebook account	€0.50
Access to compromised Gmail/French Webmail service, Spotify, or Netflix account	€1
Access to compromised Leboncon, Wi-Fi Internet service provider (ISP), Cdiscount, Pixmania, LDLC, Zalando, Auchan, or 3Suisses account	€2
Access to compromised PlayStation account (+20 games)	€3
Stolen data dump	€400
Stolen banking website config files	€50

Table 1: List of other products/services sold in the French underground

As in any other cybercriminal market, the French underground also caters to wanna-bes and newbies. A lot of cybercriminals sell training/tutorial kits to peers. The following table lists their prices in the French underground.

Training/Tutorial Topic	Price
How to open bank accounts for use in fraud	€450
How to convert credit card balances into BTC	€250
Carding	€29–150
How to convert PayPal balances into BTC	€100
SQL injection	€60
How to monetize access to compromised PayPal accounts	€60
How cybercrime affiliation works	€30
How to make an unlimited amount of Amazon refunds	€25
How to use a RAT	€20
How to send and receive illicit goods and payment anonymously	€10
How to spread malware	€2

Table 2: Training/Tutorial kits and their prices

Conclusion

Conclusion

While the French underground can't stack up to its counterparts in size and strength, its unique offerings can certainly allow it to carve its own niche in the cybercriminal economy. There isn't, after all, any other market that offers tools and services that cater to what we can consider distinctly French.

The shroud of distrust that makes the French underground market's players extremely cautious and stay very well well-hidden can pose a great challenge to law enforcement agencies and security solution vendors. But we managed to identify uniquely French constructs that cybercriminals abuse, and that's a good start. The intelligence we gather from our deep dives into criminal territory can aid law enforcement agencies and legislators in fortifying weaknesses in existing physical and legal structures. Only with continuous collaboration between the security industry and law enforcement agencies can we truly make the world safe for the exchange of digital information.

References

1. Kyle Wilhoit and Stephen Hilt. (7 December 2015). *Trend Micro Security News.* "North American Underground: The Glass Tank." Last accessed on 15 June 2016, http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/north-american-underground-the-glass-tank.

2. Trend Micro Incorporated. (1 March 2016). *Trend Micro Security News.* "Cybercrime and the Deep Web." Last accessed on 21 June 2016, http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybercrime-and-the-deep-web.

3. Max Goncharov. (28 July 2015). *Trend Micro Security News.* "Russian Underground 2.0." Last accessed on 15 June 2016, http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/russian-underground-automized-infrastructure-services-sophisticated-tools.

4. Forward-Looking Threat Research (FTR) Team. (8 December 2015). *Trend Micro Security News.* "U-Markt: Peering into the German Cybercriminal Underground." Last accessed on 15 June 2016, http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/u-markt-the-german-cybercriminal-underground.

5. Lion Gu. (23 November 2015). *Trend Micro Security News.* "Prototype Nation: The Chinese Cybercriminal Underground in 2015." Last accessed on 15 June 2016, http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/prototype-nation-the-chinese-cybercriminal-underground-in-2015.

6. Trend Micro Incorporated. (14 June 2016). *Trend Micro Security News.* "Ransomware 101: What, How, and Why." Last accessed on 21 June 2016, http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-101-what-it-is-and-how-it-works.

7. Olivier Dumons and Yves Eudes. (1 October 2015). *LeMonde.fr.* "Several Drug Sales Sites of the 'Deep Web' Pirated French (Google Translate version of: Plusieurs Sites de Vente de Drogue du «Deep Web» Français Piratés)." Last accessed on 17 June 2016, http://www.lemonde.fr/pixels/article/2015/10/01/plusieurs-sites-de-vente-de-drogue-du-deep-web-francais-pirates_4780425_4408996.html.

8. FTR Team. (12 January 2016). *Trend Micro Security News.* "Ascending the Ranks: The Brazilian Cybercriminal Underground in 2015." Last accessed on 15 June 2016, http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/brazilian-cybercriminal-underground-2015.

9. Akira Urano. (13 October 2015). Trend Micro Security News. "The Japanese Underground." Last accessed on 15 June 2016, http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-japanese-underground.

10. Sylvia Edwards Davis. (30 September 2014). *French Entrée.* "Driving Licence in France FAQ." Last accessed on 16 June 2016, https://www.frenchentree.com/living-in-france/driving/driving-licence-faq/.

11. BBC. (10 July 2012). *BBC News.* "Spy Code Creator Kills Project After Syrian Abuse." Last accessed on 16 June 2016, http://www.bbc.com/news/technology-18783064.

Created by:

TrendLabs

The Global Technical Support and R&D Center of **TREND MICRO**

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver topranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**.

TREND MICRO™

Securing Your Journey to the Cloud

www.trendmicro.com