The Internet of Things in the Cybercrime Underground

Stephen Hilt, Vladimir Kropotov, Fernando Mercês,
Mayra Rosario, and David Sancho

TREND MICRO™ | research

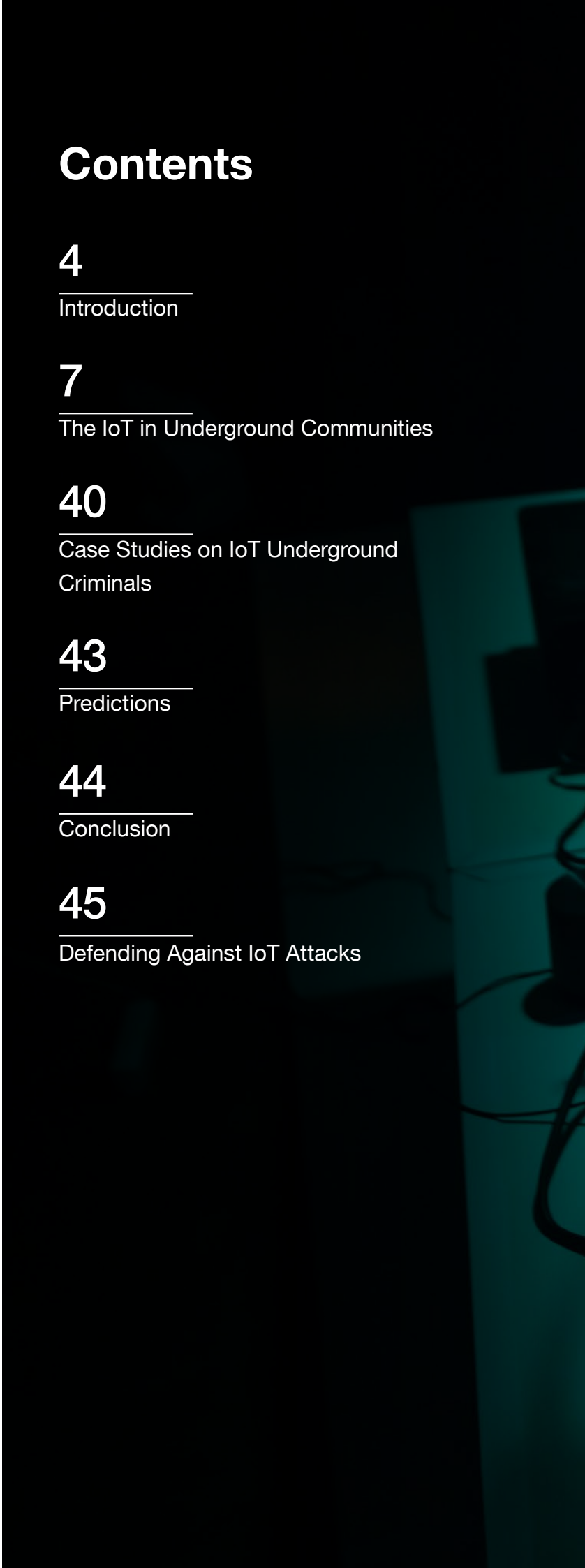
Published by
Trend Micro Research

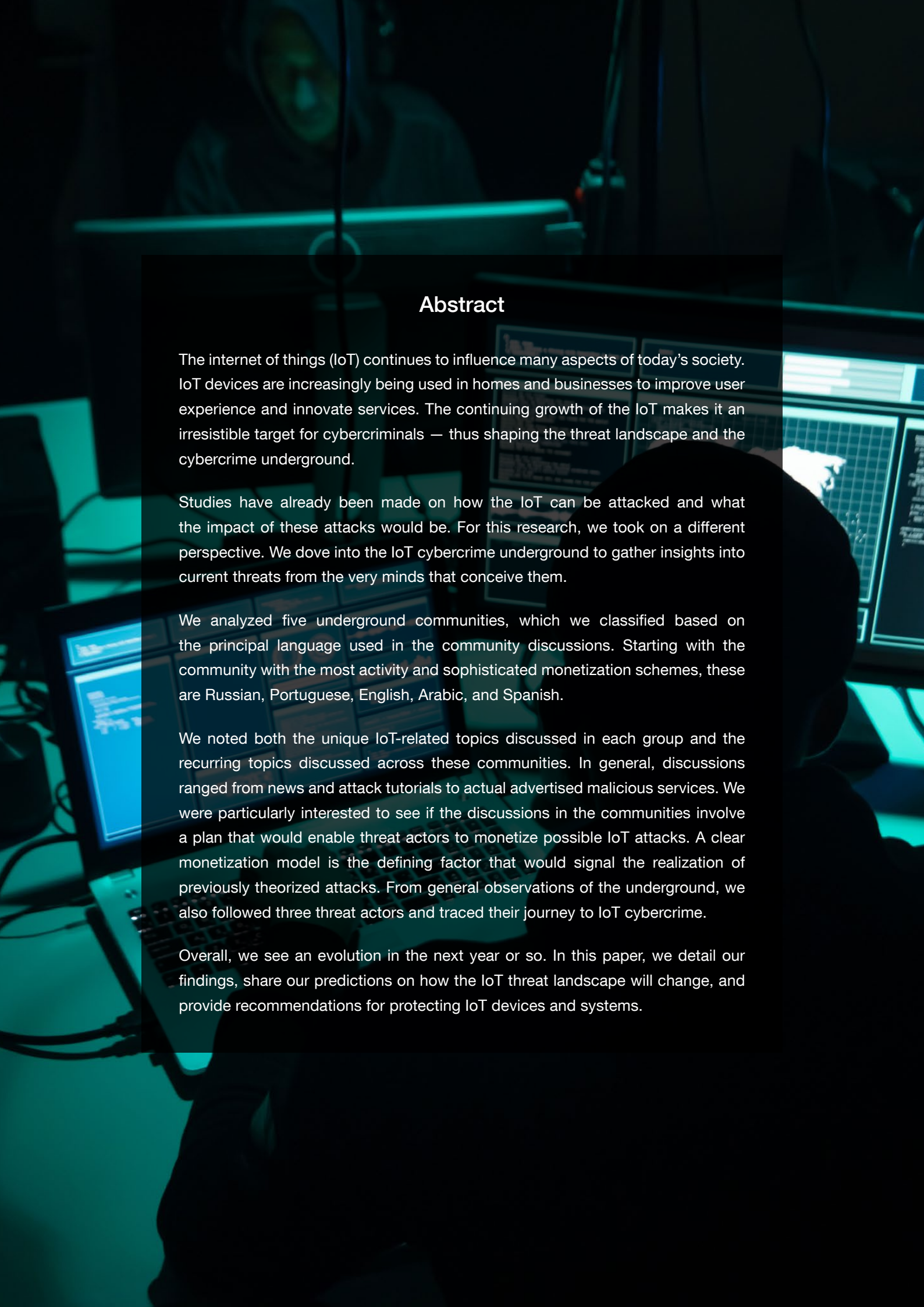
Written by
Stephen Hilt, Vladimir Kropotov, Fernando Mercês, Mayra Rosario, and David Sancho

Stock image used under license from Shutterstock.com

For Raimund Genes (1963-2017)

Contents





Abstract

The internet of things (IoT) continues to influence many aspects of today's society. IoT devices are increasingly being used in homes and businesses to improve user experience and innovate services. The continuing growth of the IoT makes it an irresistible target for cybercriminals — thus shaping the threat landscape and the cybercrime underground.

Studies have already been made on how the IoT can be attacked and what the impact of these attacks would be. For this research, we took on a different perspective. We dove into the IoT cybercrime underground to gather insights into current threats from the very minds that conceive them.

We analyzed five underground communities, which we classified based on the principal language used in the community discussions. Starting with the community with the most activity and sophisticated monetization schemes, these are Russian, Portuguese, English, Arabic, and Spanish.

We noted both the unique IoT-related topics discussed in each group and the recurring topics discussed across these communities. In general, discussions ranged from news and attack tutorials to actual advertised malicious services. We were particularly interested to see if the discussions in the communities involve a plan that would enable threat actors to monetize possible IoT attacks. A clear monetization model is the defining factor that would signal the realization of previously theorized attacks. From general observations of the underground, we also followed three threat actors and traced their journey to IoT cybercrime.

Overall, we see an evolution in the next year or so. In this paper, we detail our findings, share our predictions on how the IoT threat landscape will change, and provide recommendations for protecting IoT devices and systems.

Introduction

The internet of things (IoT) has become a catchall phrase for the growing trend of connecting various forms of devices to the internet among manufacturers and integrators. Sometimes, internet connectivity is a useful feature to incorporate in new hardware. For example, a fitness device that collects health information can send it straight to the cloud, or a standalone home camera can stream real-time footage the owner can access from the office.

In some cases, however, vendors just connect devices without adding the required security measures — a dream scenario for hackers and other attackers. Having direct access to all manner of equipment allows cybercriminals to take over these internet-enabled machines much more easily. Once the device is "pwned," a hacker can steal the data it holds or perhaps use the device as an attacking platform against other victims.

Often, a weak security configuration is what allows an attacker a way into the device. For instance, online cameras that use a predictable password or have no authentication at all are relatively common. Other times, certain devices are found online when they shouldn't be. This is patently absurd when it happens to industrial equipment in a manufacturing or healthcare environment, such as factories and hospitals. These industrial machines should instead use a virtual private network (VPN) connection if they need to be accessed remotely. Aside from the use of VPN, there are a number of secure configurations that will not require these devices to be directly exposed to the internet at large. It is recommended that integrators always follow their industry's best practices when it comes to the IoT.

Furthermore, pedestrian applications of the IoT can suffer from the same problem. For instance, internet-connected home or office printers don't make a lot of sense, as these kinds of machines should not be inadvertently exposed to the internet. If a user requires remote printing, there are a number of more secure options, such as Cloud Printing Services or a secure VPN.

When used for connected devices, routers can also be considered as IoT devices. Home and office routers have been prevalent for many years and from our experience, they are still the most frequently attacked IoT device. Therefore, if this trend were to remain unchanged, routers are the most prone to future attacks. Attackers consider routers as IoT devices because they are possible entry points for an attack. This is why, in this paper, we will count them as IoT devices as well.

This is not to say that there has not been any effort done to acknowledge the threats and challenges to the IoT. IoT doomsday scenarios have been discussed in the media before, but these attacks remain theoretical until the bad guys start targeting real victims. The main concern with these attacks is that, for them to become commonplace, cybercriminals need to find a viable business model.

That is why, in this research, instead of outlining potential attacks, we surveyed online criminal forums to gauge the level of interest and possible business models there may be for IoT-specific attacks. The main interest of our research was to find out what hackers and criminals think of in terms of attacks on existing IoT infrastructure.

In scouring underground forums and communication platforms, we were able to discern an average profile of cybercriminals discussing IoT-related topics. At this point, we can confidently say that, in general, IoT attacks are not made by professionals trying to subvert IoT infrastructure. Instead, they are made by typical old-time cybercriminals who have evolved into IoT attackers.

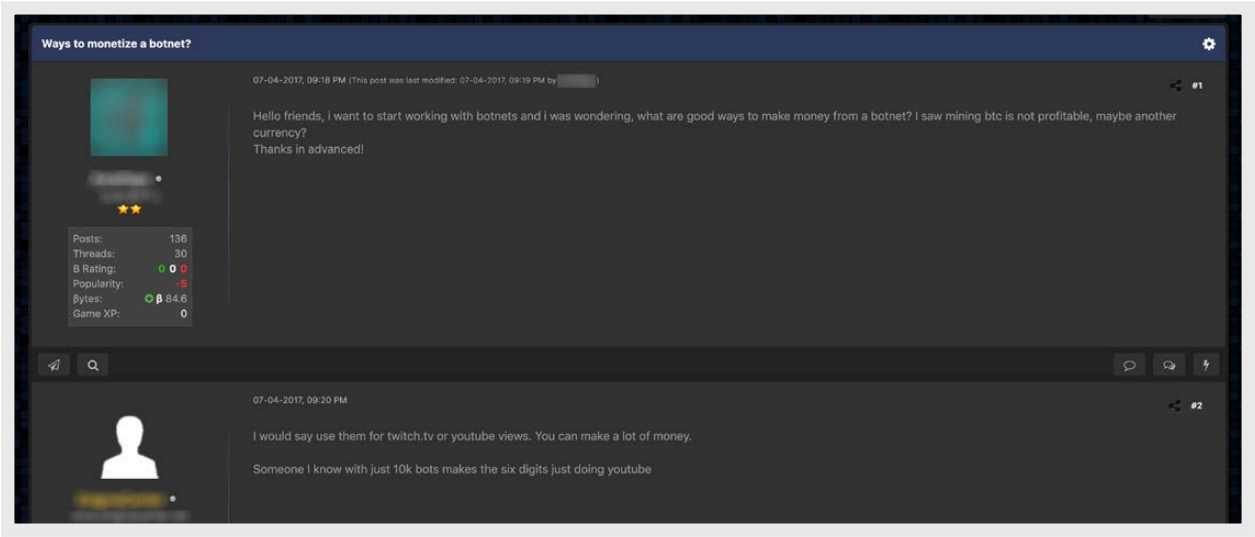


Figure 1. Hack Forums discussion on how to monetize IoT botnets

We saw a lot of interest in and curiosity about a wide variety of online devices. The most requested hacking methods were for routers, webcams, and printers.

There were also tutorials on the inner workings of commercial gas pumps, including programmable logic controllers (PLCs). PLCs are devices found in factories and other structures with industrial machinery that enable complex equipment to be managed remotely. Along with mere tutorials, we also saw tools for discovering and exploiting online devices, which were again mostly routers and webcams.

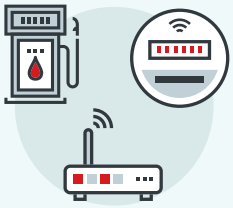
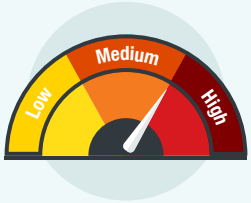
The most common way to monetize router infections is to set up botnets, which can later be used as a distributed network that provides services that can be offered to other criminals for a fee. Webcams, on the other hand, are usually monetized by selling access to their video streams. As expected, the price for stream access and buyer interest depend on where and what the camera is looking at. The most prized streams are bedrooms, massage parlors, warehouses, and payment desks at retail shops. These video streams are often categorized thematically and sold as subscriptions.[1]

Another popular offering is either software for or tutorials on automating searches for specific devices on Shodan, which is a very popular web search engine for finding online devices.

We have given a few examples of what we saw while scouring underground forums to provide an overview. The next sections provide an in-depth look at what each criminal underground community offers to criminals interested in attacking IoT devices and infrastructure. We have classified these communities according to the language they use, as it is a unifying marker of each community more so than geographical location. We chose five languages which have communities we consider are among the top players in the underground community: Russian, Portuguese, English, Arabic, and Spanish.

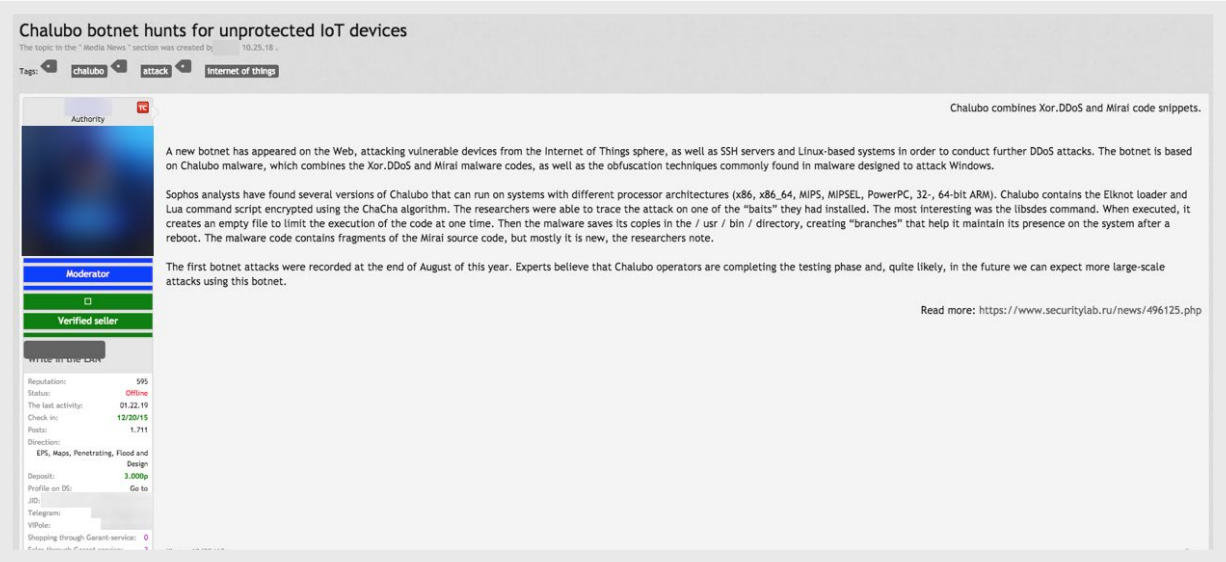
The IoT in Underground Communities

Russian Underground Communities

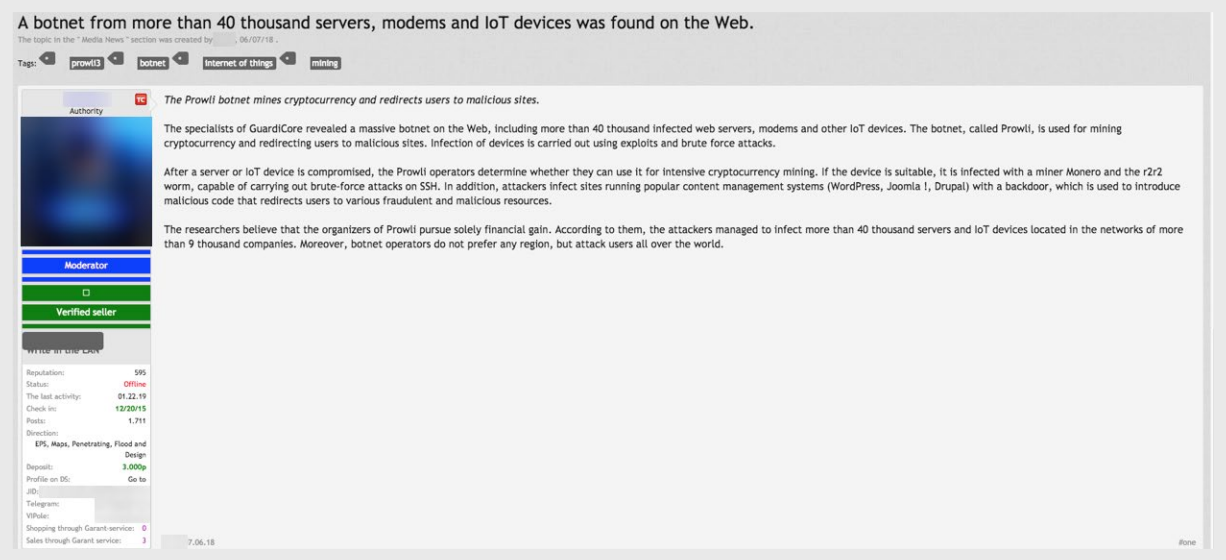
Devices Targeted	Marketplace Monetization Level	Outlook
		
Routers, smart meters, gas pumps	Medium/High	Focus on monetization, curiosity about less common platforms

The Russian cybercrime underground market is the most sophisticated out of all the underground communities we discuss in this paper. The money-driven criminals make up a market thriving with exploits for routers, customized firmware for smart meters, talks of hacking gas pumps, and router-based botnets for sale. There is a variety of conversations taking place around devices, including less common platforms. Most of these talks have a monetization angle. In general, the Russian underground is a place for business where hacking and technical information are mere details.

Users in the Russian underground are interested to know the latest news about IoT attacks sourced from the information security world, as seen in Figures 2 and 3.



Post about an IoT botnet being used for distributed denial-of-service (DDoS) attacks



Post about a cryptocurrency-mining botnet

Figure 2. A user sharing news about IoT botnets found by security companies

Figure 3. A user sharing news headers that the Russian company Fizpribor was offering a bounty for any hacker that can enter its network

The Russian underground is a dynamic place where all sorts of illegal and shady products are up for sale. Criminals often post advertisements looking for IoT botnet developers. In addition, other users ask for things they are ready to buy. In the sample in Figure 4, the user is offering money in exchange for vulnerabilities specifically in IoT devices and routers.

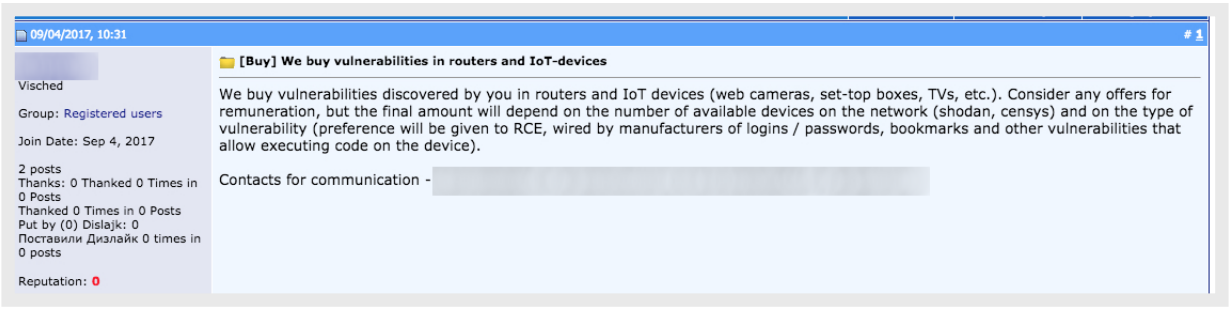


Figure 4. A user asking for exploitable vulnerabilities in IoT devices

We think it's important to note how new developments in Android technology are affecting IoT devices and their potential to become infected, something especially demonstrated in the Russian community. For instance, we have seen an Android cryptocurrency miner being offered on these Russian forums. For cybercriminals, this kind of malicious software will likely not be used for targeting phones since it would deplete batteries too quickly. Cybercriminals will probably target Android-based IoT devices instead. For instance, smart TVs and similar devices are commonly Android-based, and these seem to be better targets for a cryptocurrency miner than smartphones.

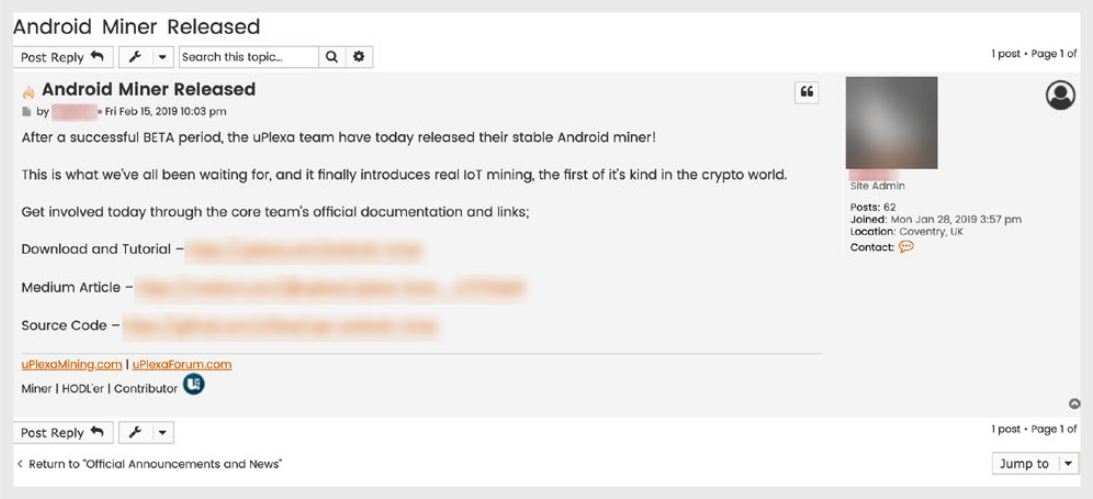


Figure 5. Advertisement selling a new IoT Android cryptocurrency miner

The Russian cybercrime underground markets have monetization schemes not only for router-based botnets but also for hacked cameras. Aside from these more common devices, forum members are also looking into hacking smart electricity meters. The Russian government has recently mandated that all electricity meters be replaced by online smart meters, which explains the proliferation of meter hacking. Of course, Russian hackers and criminals are already looking into modifying and selling customized firmware for these new devices. So far, there doesn't seem to be a clear monetization plan for this beyond physically selling modified smart meters. These modified smart meters are marketed as a means to save on monthly residential bills for electricity, water, and gas.

In the future, hacking smart meters may offer criminals a new way of making money. Nowadays, attacking these devices is probably more akin to hacktivism rather than professional money-driven attacks.

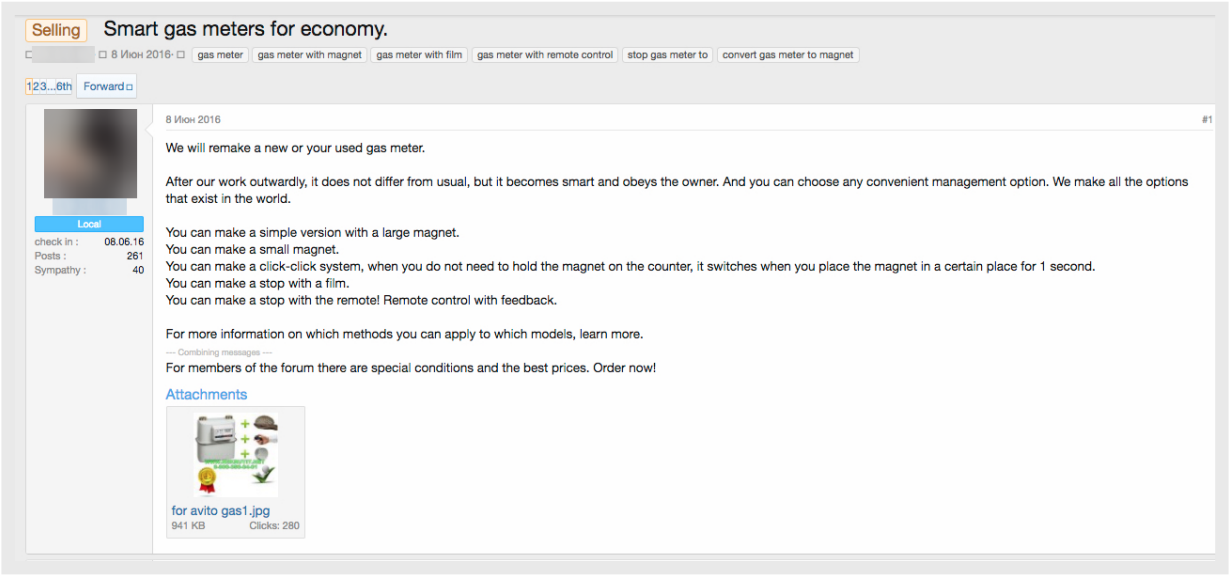


Figure 6. A post selling modified smart gas meters

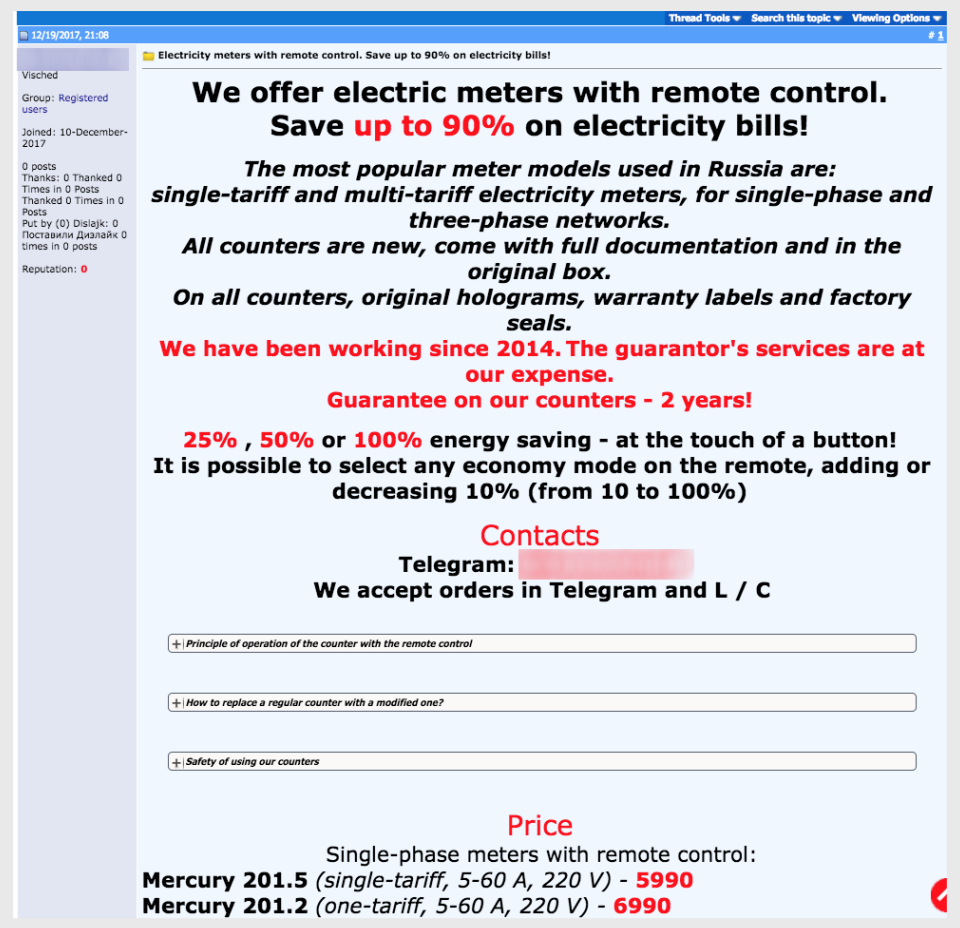


Figure 7. Two posts selling modified smart electricity meters

Recently, a new Linux ransomware that targets network-attached storage (NAS) systems has surfaced in the forums as well. This may be a big deal for companies which rely on such devices to store corporate data. This also brings forward a new monetization scheme for IoT devices, but since this is a new development, we cannot know how effective it is and, therefore, whether it will establish a new trend for IoT attackers.

In general, the main methods of monetizing IoT botnets on the Russian cybercrime underground are the following:

- Using infected devices to launch DDoS attacks
- Using infected devices as VPN exit nodes

In both cases, the criminals end up selling the services to other criminals in their community. The images in Figures 8 and 9 are examples of both of these monetization schemes.

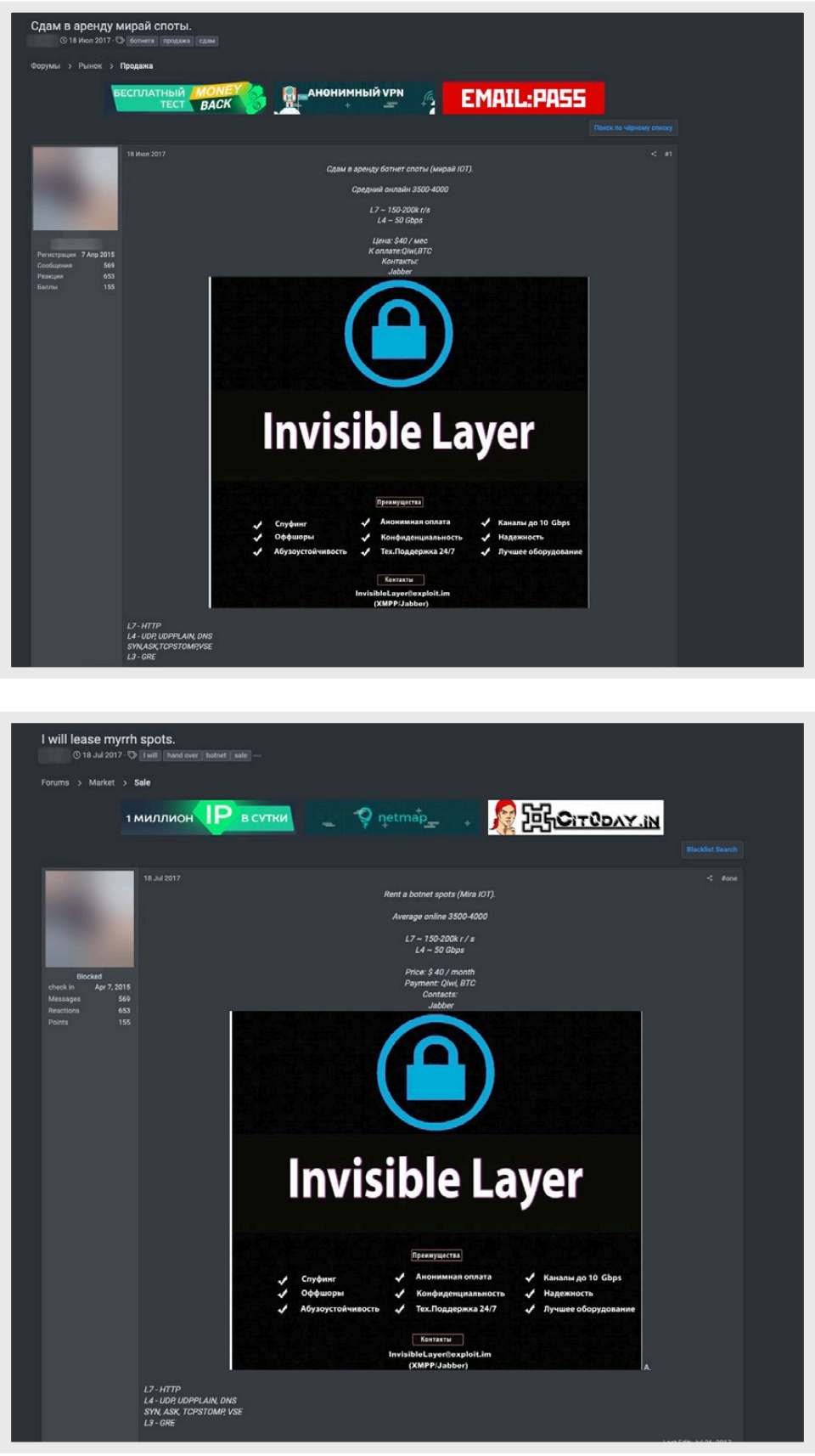


Figure 8. A post in Russian offering DDoS services based on infected IoT devices at US$40 per month (top) and the translated version (bottom)

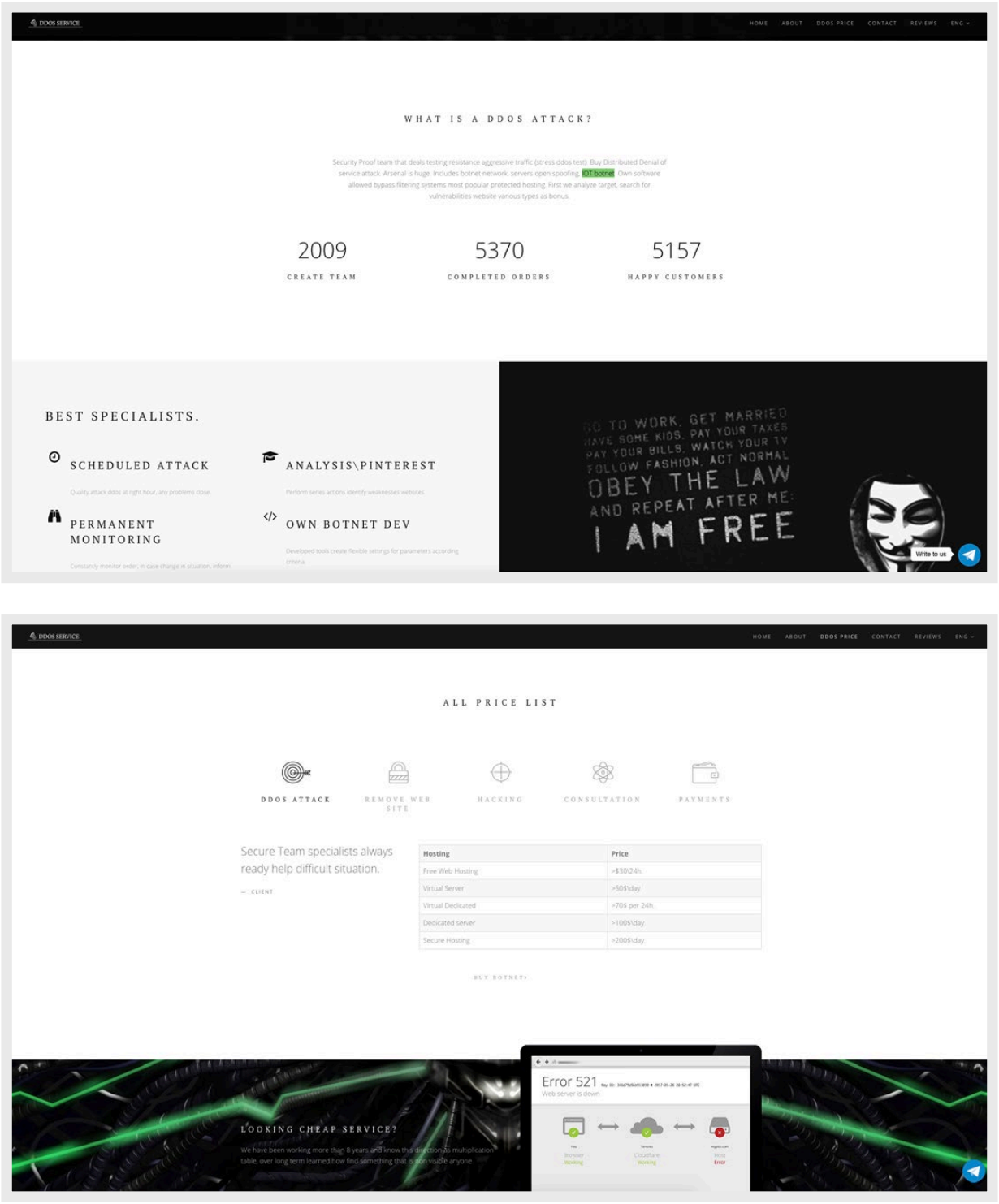


Figure 9. Webpage in English offering DDoS services specifying the use of an IoT botnet (top); pricing is based on the target of the attack (bottom)

The second way of monetizing infected devices is by making them act as exit nodes of a VPN network that criminals sell as a service to other criminals.

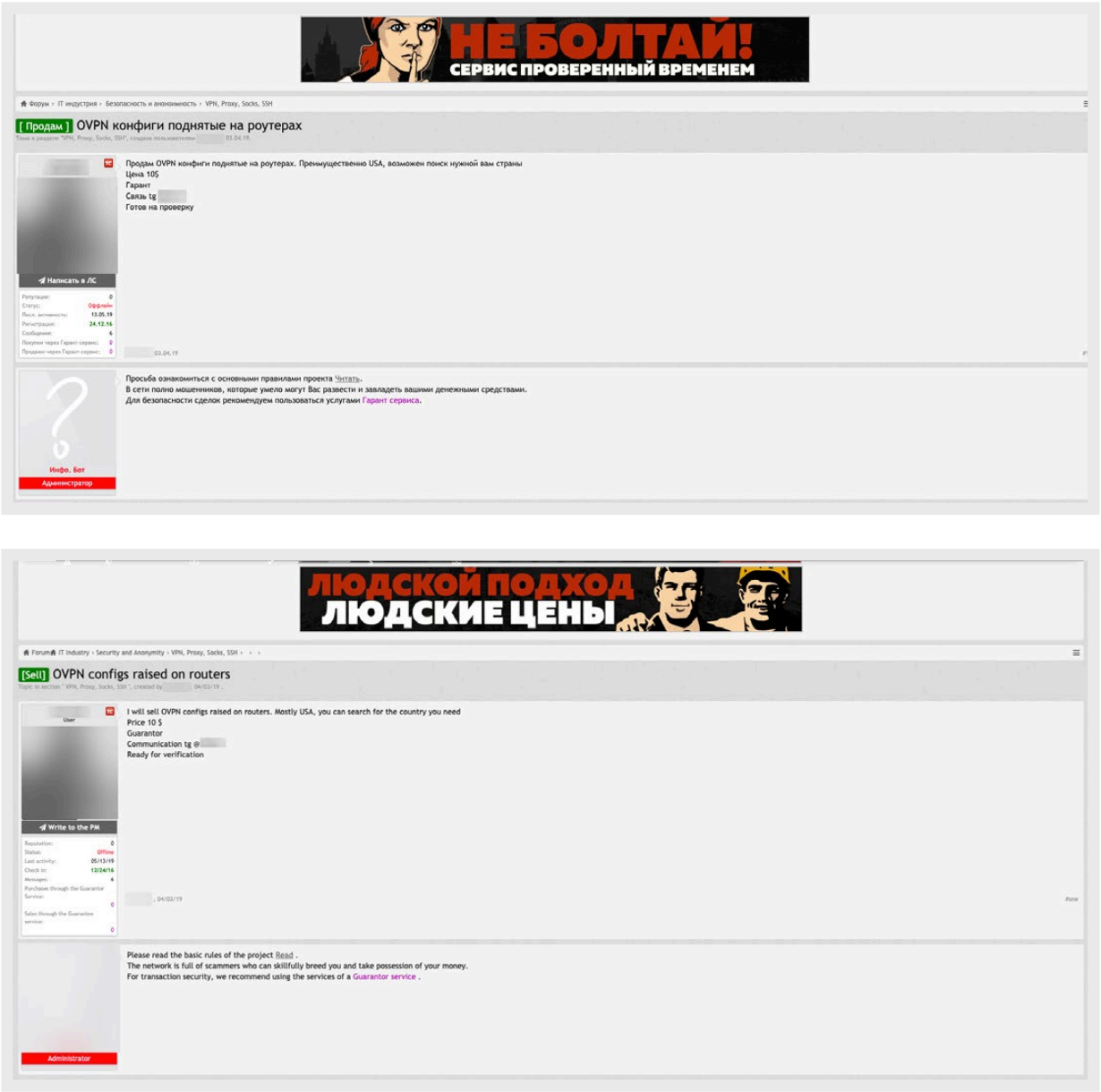
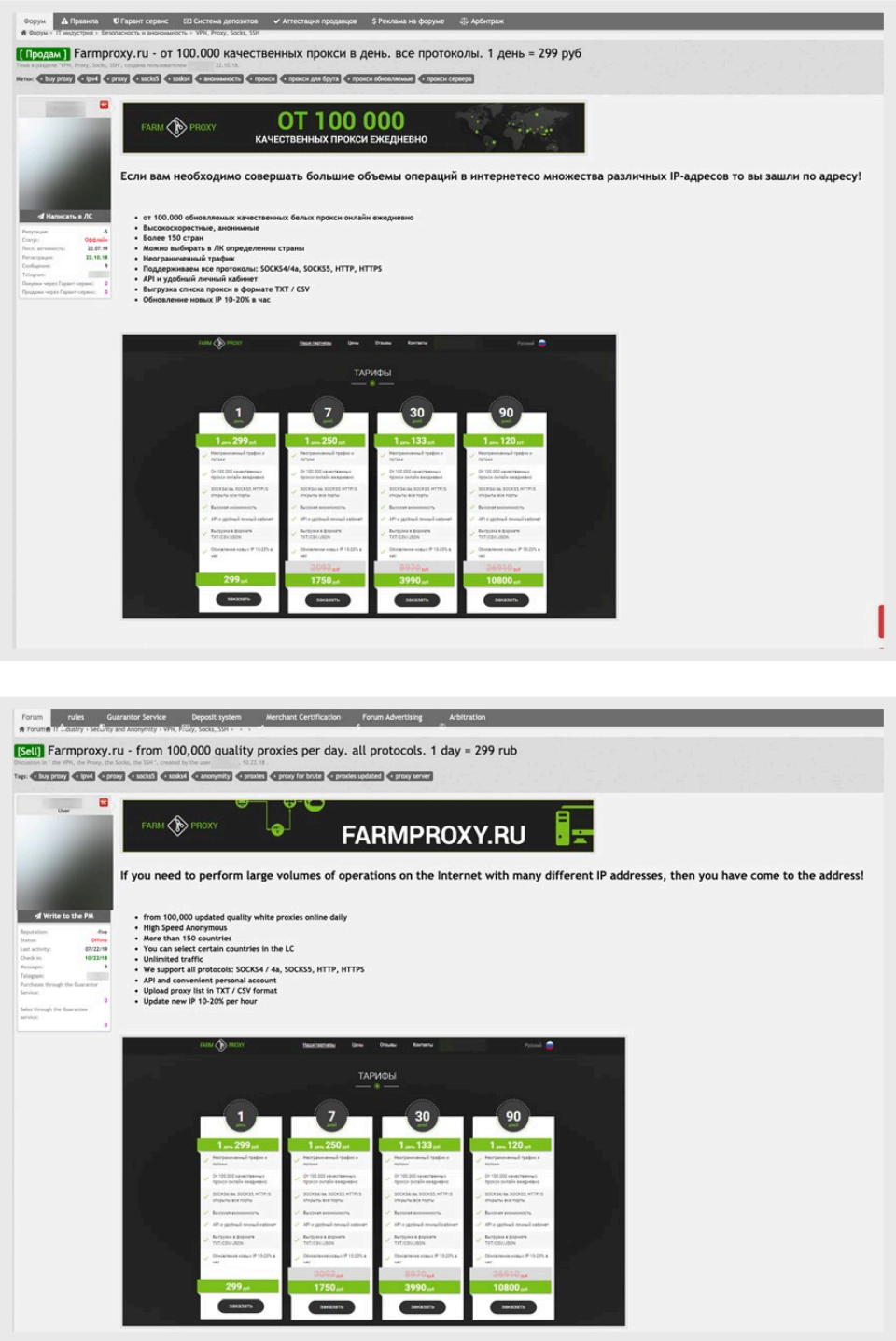


Figure 10. A post in Russian selling an IoT-based VPN (compromised router with OpenVPN) for US$10 per proxy (top) and the translated version (bottom)



Note: The ad puts the price at 299 Russian roubles per day (or US$5), with pricing for other packages for seven, 30, and 90 days of operation.

Figure 11. Advertisements in English (top) and Russian (bottom) for a big proxy pool of about 100,000 hosts consisting mostly of compromised routers

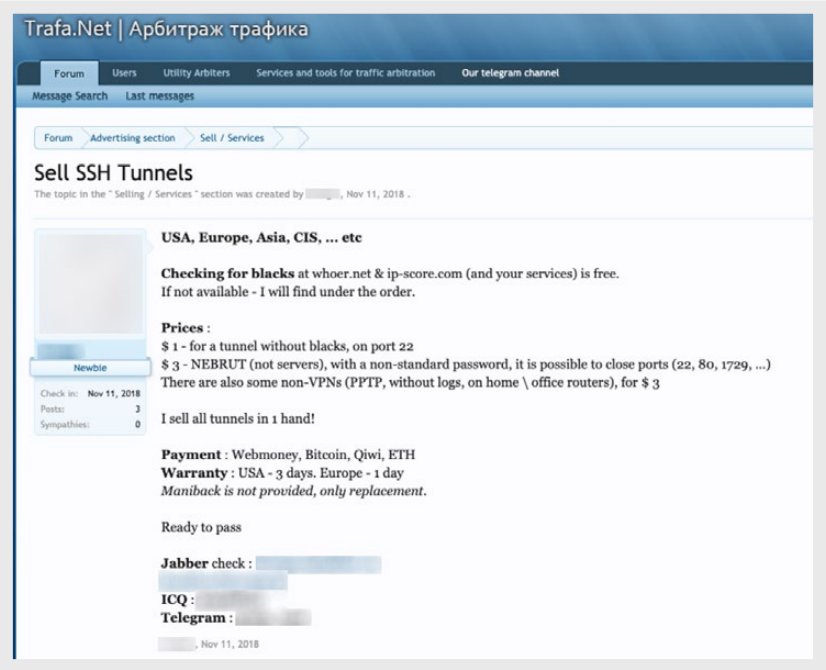


Figure 12. A post advertising a VPN service where the author mentions specifically that the nodes are “home / office routers”

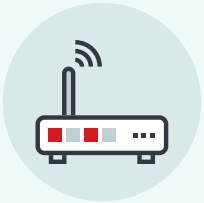
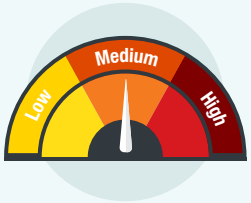
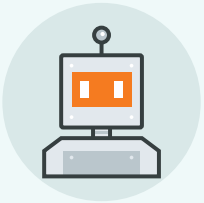
Service	Price
Modified smart gas meters	Approximately US$93 and up
Modified smart electrical meters	Approximately US$92 and up
Shodan access	US$25
DDoS service based on compromised IoT devices	US$40 per month
IoT-based VPN	US$1 to US$10 per compromised router, depending on the quality of the IP reputation

Table 1. Prices of the services found in the Russian underground forums

In these online forums, we also saw discussions about gas pumps, but those are in the early stages and so far lack a clear monetization plan beyond selling the physical modified devices.

In general, cybercriminals in the Russian underground have the ability and the opportunity to develop IoT attacks. Most notably, they have found ways to monetize hacking IoT devices.

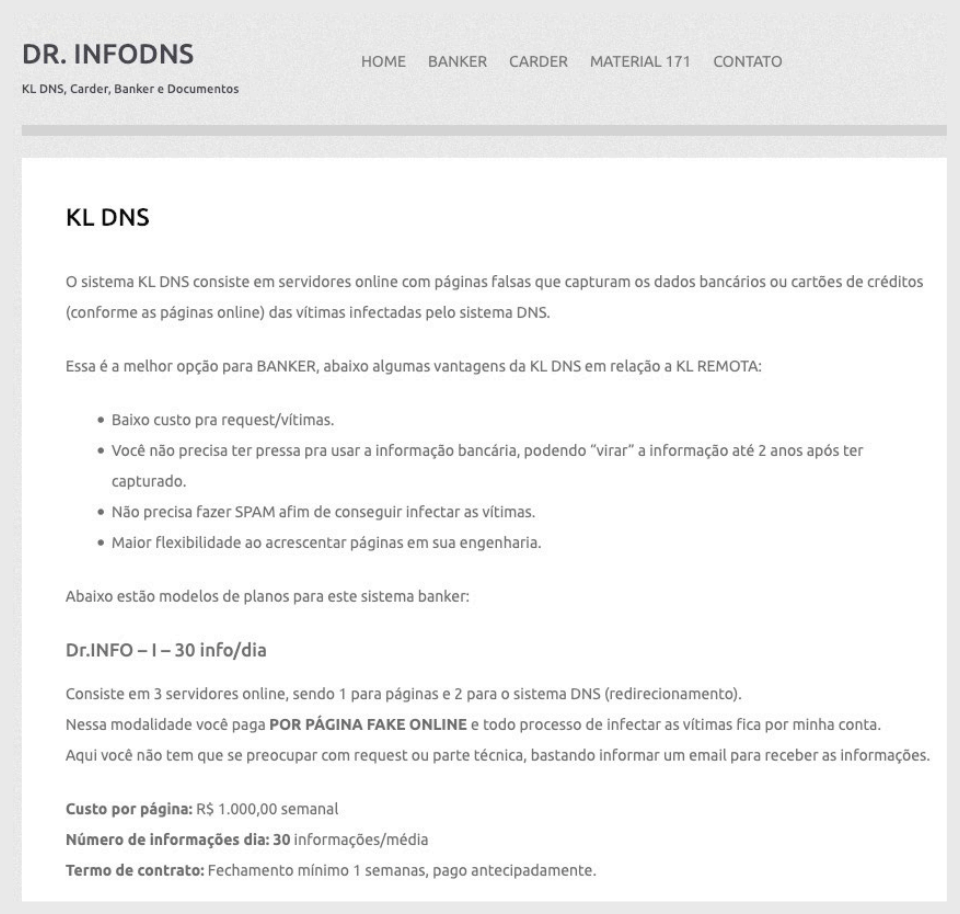
Portuguese Underground Communities

Devices Targeted	Marketplace Monetization Level	Outlook
		
Routers, ADSL and cable modems	Medium	Information exchange, router botnet monetization

The Portuguese-speaking criminal underground is composed of web forums mostly populated by Brazilian users. These users also connect through some other private chat rooms, for example, Telegram, WhatsApp, and Discord. We saw requests for information and hacking tutorials. But the most interesting ads we saw are those for services that use infected routers and similar devices as the basis for further criminal services. This is the case for "KL DNS," which is a kind of service sold on Brazilian forums to perform foolproof phishing campaigns combined with DNS redirection and, in some cases, SMS spamming.

"KL DNS" services start with a network of infected routers or other home devices. The criminals change the DNS configuration on these devices so that the name resolution is done by a hacker-controlled external server. From that point on, when a computer within the infected device's network tries to resolve, for example, "bank.com," the browser would instead redirect the request to a phishing site that looks identical to the real bank website. Attackers can do this for as many banking websites as they want or as many other legitimate sites, setting up a target user to fall into a phishing trap.

The main selling point of this system is that, for it to work, it would not need to infect a victim's computer, only the internet-connected router. The criminals sell these redirection services so that phishers can host copycat web servers and gather stolen credentials and credit card information. Prices are around R$1,000 per week (about US$260), as shown in the samples in Figures 13 and 14.



DR. INFODNS

KL DNS, Carder, Banker e Documentos

HOME BANKER CARDER MATERIAL 171 CONTATO

KL DNS

O sistema KL DNS consiste em servidores online com páginas falsas que capturam os dados bancários ou cartões de créditos (conforme as páginas online) das vítimas infectadas pelo sistema DNS.

Essa é a melhor opção para BANKER, abaixo algumas vantagens da KL DNS em relação a KL REMOTA:

- Baixo custo pra request/vítimas.
- Você não precisa ter pressa pra usar a informação bancária, podendo "virar" a informação até 2 anos após ter capturado.
- Não precisa fazer SPAM afim de conseguir infectar as vítimas.
- Maior flexibilidade ao acrescentar páginas em sua engenharia.

Abaixo estão modelos de planos para este sistema banker:

Dr.INFO – I – 30 info/dia

Consiste em 3 servidores online, sendo 1 para páginas e 2 para o sistema DNS (redirecionamento).
Nessa modalidade você paga **POR PÁGINA FAKE ONLINE** e todo processo de infectar as vítimas fica por minha conta.
Aqui você não tem que se preocupar com request ou parte técnica, bastando informar um email para receber as informações.

Custo por página: R$ 1.000,00 semanal
Número de informações dia: 30 informações/média
Termo de contrato: Fechamento mínimo 1 semanas, pago antecipadamente.

Translation:
The KL DNS system that consists of online servers hosting fake webpages to capture bank account information or credit cards of infected victims.

This is the best option for BANKERS (people involved with bank digital frauds). The following are some of its advantages over traditional banking Trojans:

- Low cost per request/victims
- You don't have to rush the use of the captured bank information, so you can use it up to 2 years after capturing it
- You don't need to spam victims
- Offers better flexibility when adding your own fake webpages

The following are the buying options for this system:

30 victims per day

3 online servers: 1 for hosting the fake webpages and 2 for the DNS redirect system. Choosing this option, you pay via a fake page wherein all the victim infection process will be up to me. In this option you won't have to worry about the technical aspects. You would only need to provide me an e-mail where I can send the captured data to.

Cost per page: R$ 1,000.00 weekly
Average number of victims: 30
Contract terms: at least one week, paid in advance

Figure 13. Advertisement for a "KL DNS" service

Translation:
Here you find the best KL DNS system in the market. We offer you two options for availing it: with or without our infection services.

In our completed and advanced DNS management system, our team is 100% responsible for the management, setting up and guarantee of the outcome from our system. You're only responsible for monitoring the email for the captured data.

We also have an option that includes SMS SPAM with more flexible costs, but that's a simpler system which would have different results from the advanced DNS management system.

Figure 14. Advertisement for a "KL DNS" service with two different price variants

The KL DNS criminal service takes advantage of router infections for financial gain. The target audience is other criminals that already host phishing sites. This is clearly a sign of rising professionalism in the IoT space. These criminals have figured out a way to make money off of infected devices by creating a service that they then sell to other criminals. The existence of these business models power dynamic criminal marketplaces. There are other ways these markets may become more complex, and we believe this to be the first sign of what is coming.

The precursor to KL DNS may have been the mass infection of MikroTik routers through a vulnerability, which took place in the first half of 2018 in Brazil.[2] An attack of this magnitude is still very possible, with criminals certainly on the lookout for new vulnerabilities and attacks against IoT infrastructure.

As for the posts on IoT hacking in the Portuguese underground community, the most notorious one we saw was an in-depth technical tutorial on how to hack gas pumps. It even included links to official documentation and step-by-step explanation.

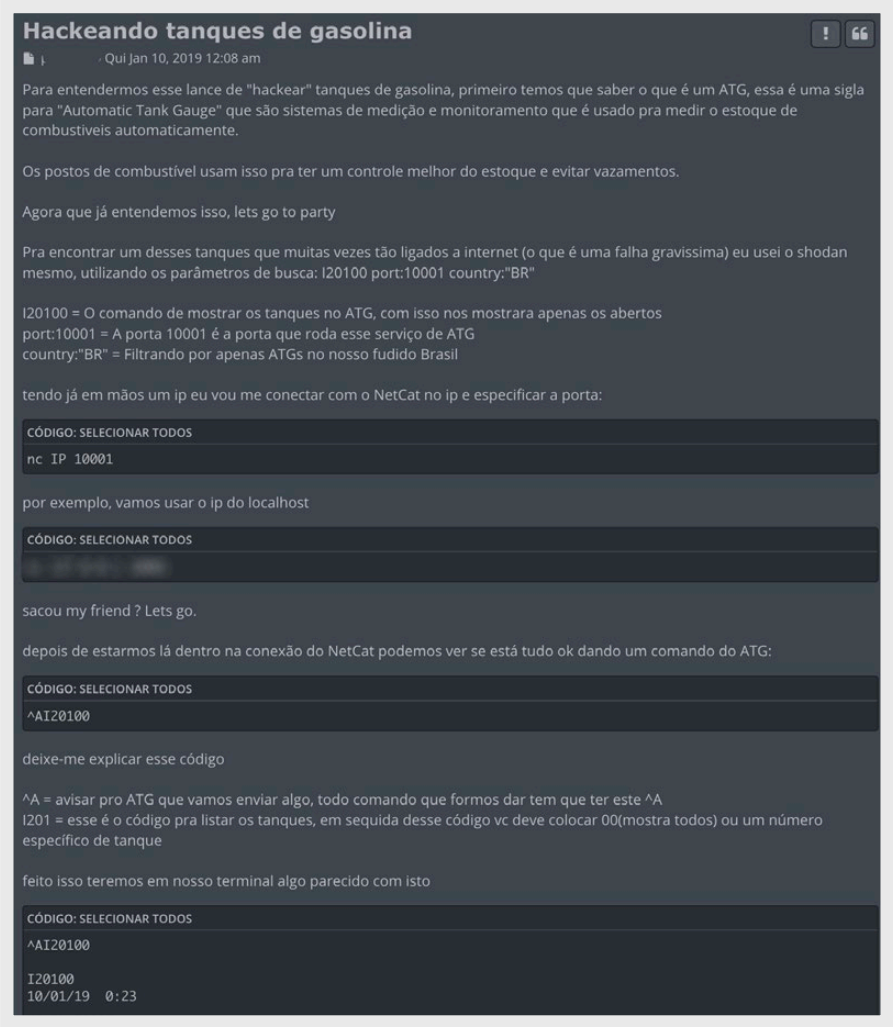


Figure 15. A step-by-step tutorial on hacking gas pumps

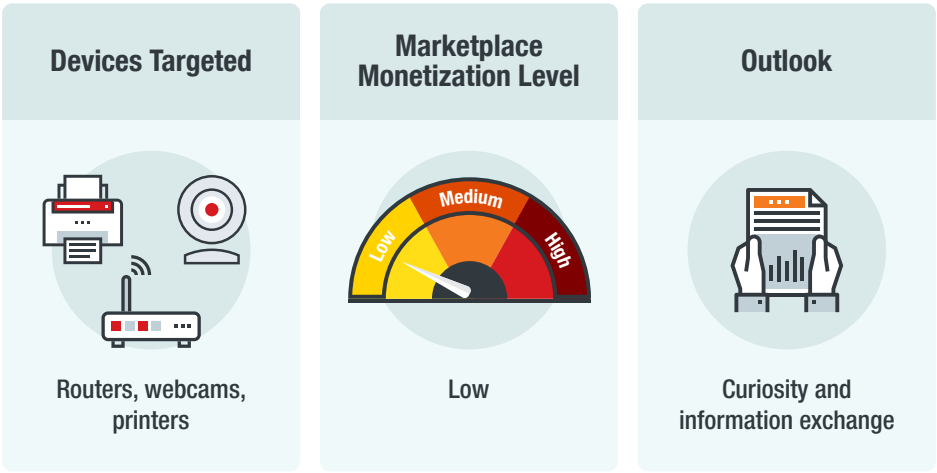
Figure 15 shows a discussion in the Brazilian underground about hacking gas pumps. It's a full tutorial that teaches how to find and connect and send commands to a specific gas pump model. The topic author teaches those in the forum how to change a tank name to "cashew juice" as an example.

Attacks on gas pumps are something we've discussed in an earlier research in 2015. In the paper, we discussed how supervisory control and data acquisition (SCADA) and industrial control systems (ICS) in such a context could be tempting targets for attackers and outlined the implications of inadequate security on them.[3]

Service	Price
DNS service	US$259 weekly

Table 2. Price of the KL DNS service found in the forums

English Underground Communities



Equivalent communities in the English-speaking world could be more accurately described as hacking forums, as opposed to being criminal in nature — but some criminality can be seen. On the hacking forums we found tutorials on how to attack and exploit a variety of devices.

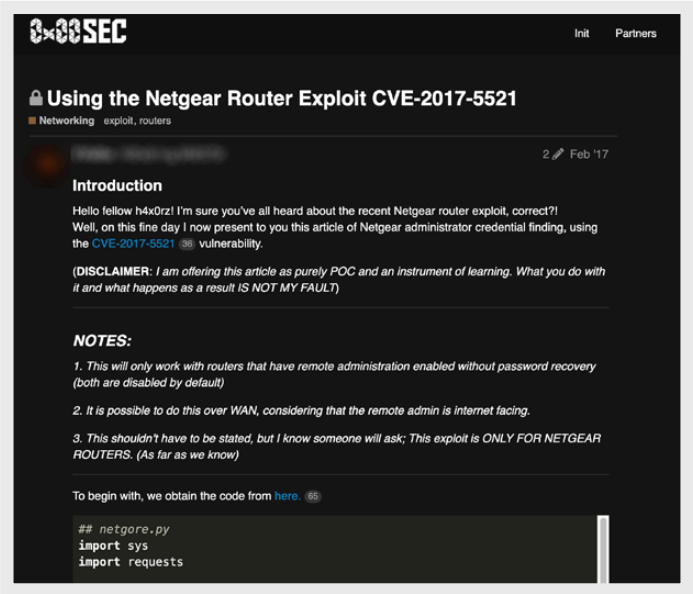


Figure 16. Hacking forum tutorial on how to exploit a security vulnerability of routers from a particular brand

The most talked about devices in this community are routers and webcams. These are the most common and well-known devices that hackers and other criminals are interested in targeting. We also saw an interest in attacking printers, perhaps due to how ubiquitous they are in offices and corporate environments. They also tend to be unprotected and unmonitored.

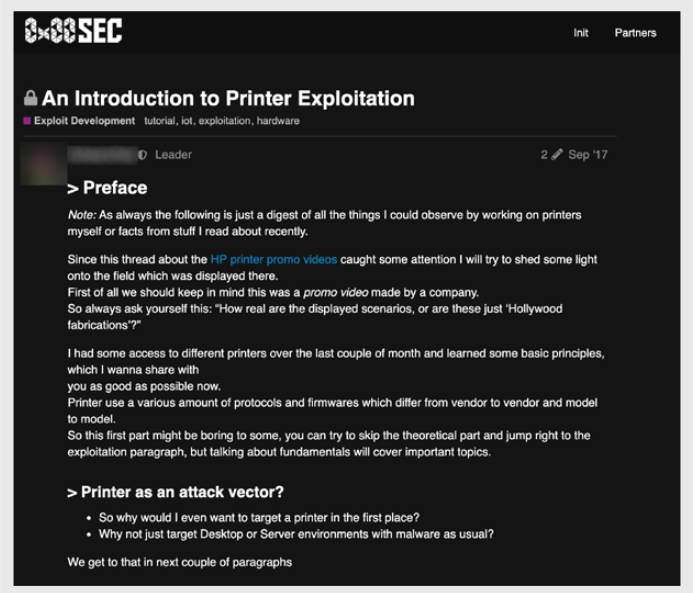


Figure 17. Hacking forum tutorial on a generic printer exploitation

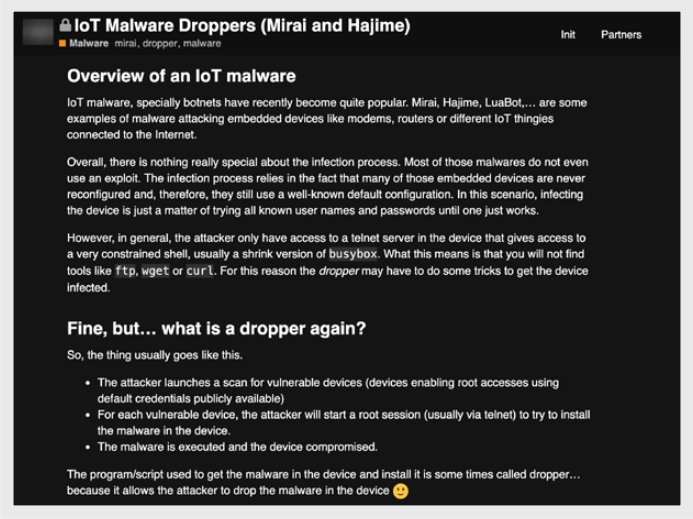


Figure 18. Hacking forum tutorial on setting up a malware dropper to infect routers

Besides webcams, routers, and printers, we noticed an interest in other less common devices. For instance, we saw a forum where users shared "aztarna," an automated discovery tool for industrial robots that is commonly used for legitimate purposes. These kinds of requests are sparse, but they certainly do exist. Other discovery tools are much more common, such as those for routers.

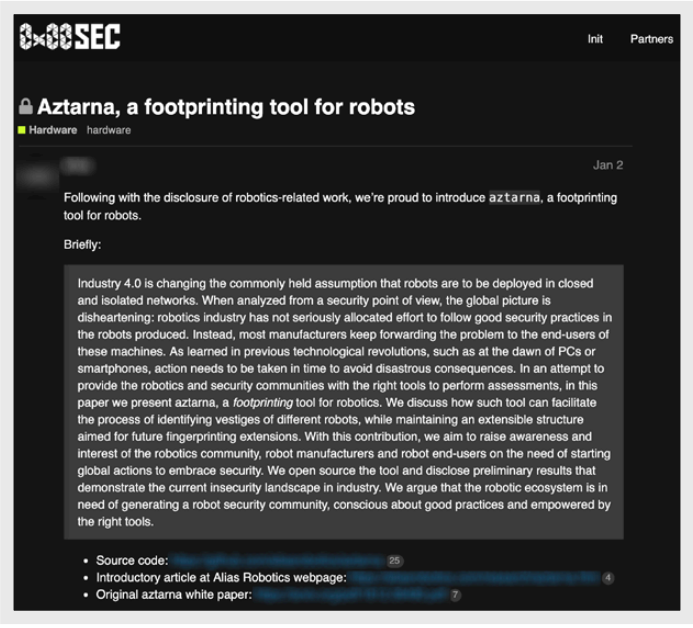


Figure 19. Hacking forum post about a free tool for discovering industrial robots

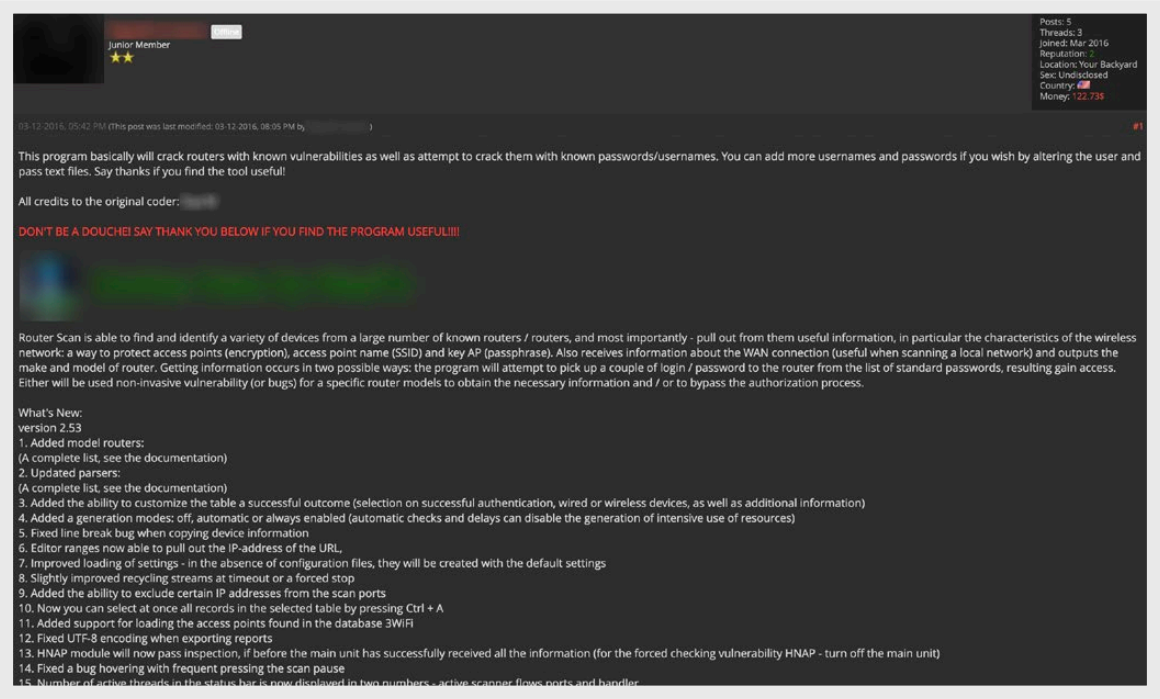


Figure 20. A post about a free tool for discovering routers

Not only did we see discovery toolkits, actual exploits, and canned attacks for certain devices, but we also saw cybercriminals' attacking tools in some cases and the actual exploit code in others.

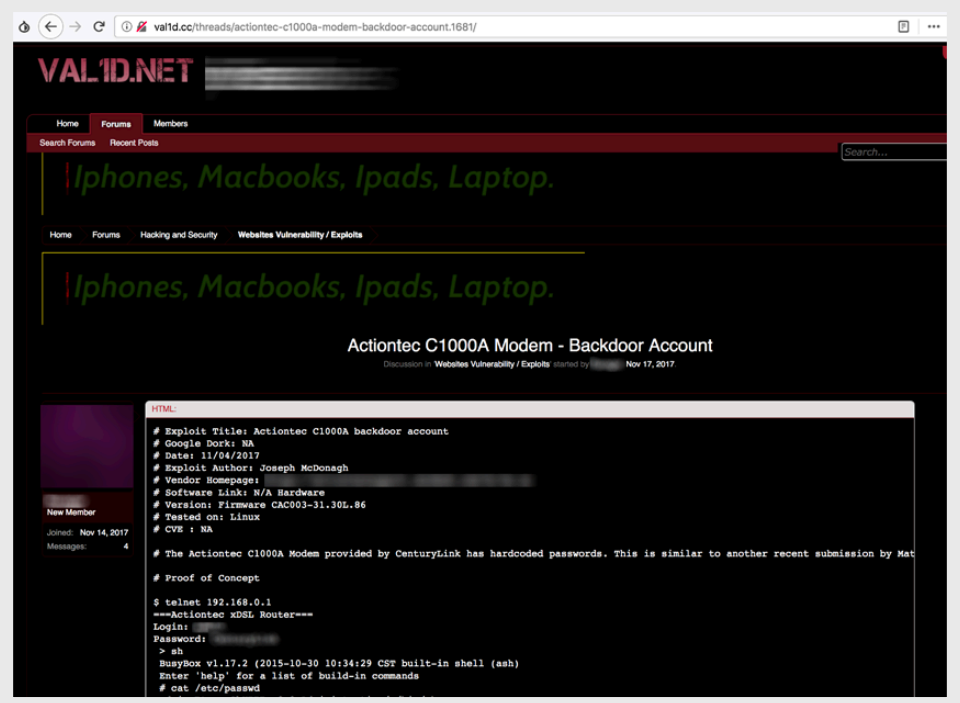


Figure 21. Post sharing an exploit for a particular online device

We noticed one topic that popped up often in these criminal environments: the results of an attacker having already broken into devices and infrastructure. If hackers manage to break into an ICS application, they may try to sell this access to anyone who may be interested in taking full advantage of the application. The same thing can be said for IoT botnets that hackers have not been able or are not willing to monetize. Access to these botnets is offered wholesale on English underground forums.

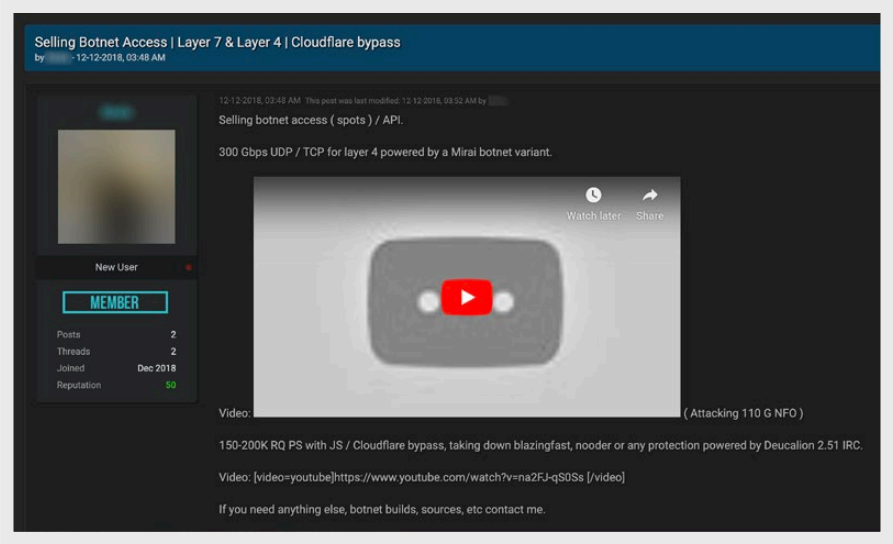


Figure 22. A user selling Mirai botnet rentals on Nulled

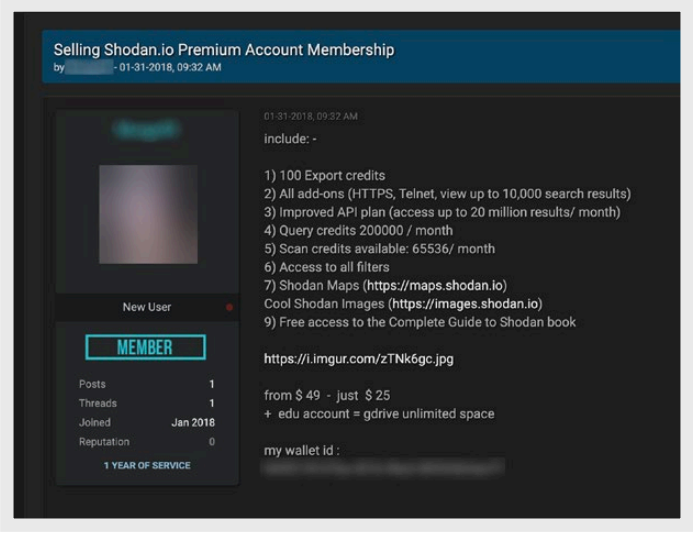


Figure 23. Shodan accounts for sale on Nulled

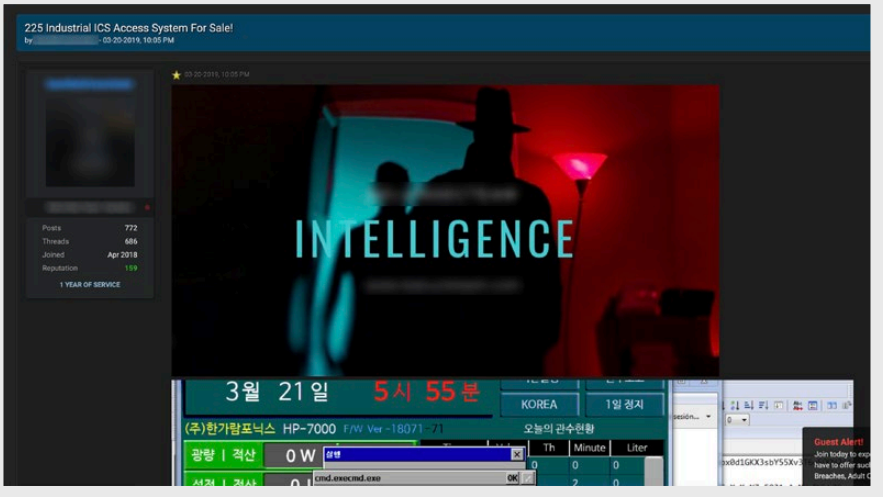


Figure 24. ICS access for sale on Raidforums

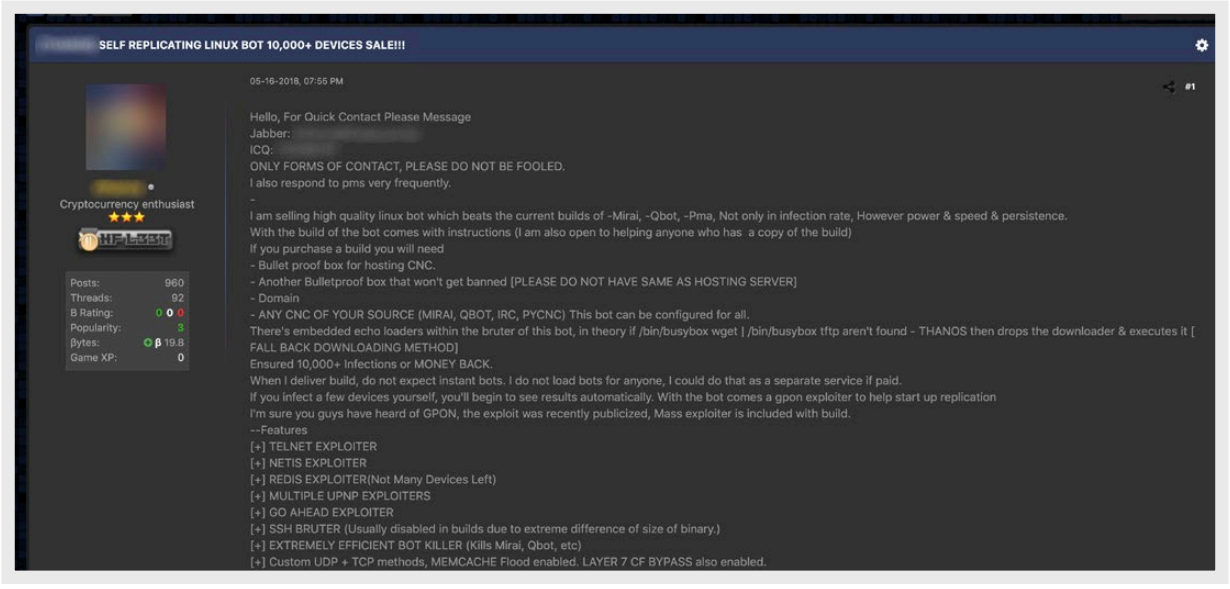


Figure 25. IoT botnet for sale on Hack Forums

When talking about IoT botnets, Mirai is, of course, an important piece of the puzzle. After its code became open source back in 2016, Mirai has become the gold standard for the mass infection of routers. More often than not, Mirai is somehow involved in discussions about IoT infections in general. That is why it's not surprising that Mirai source code modifications are common in these forums as well.

We have seen criminals selling consulting services to other criminals to help them configure their own Mirai botnets. Qbot, a precursor to the much more popular Mirai, is also shared, though less often.

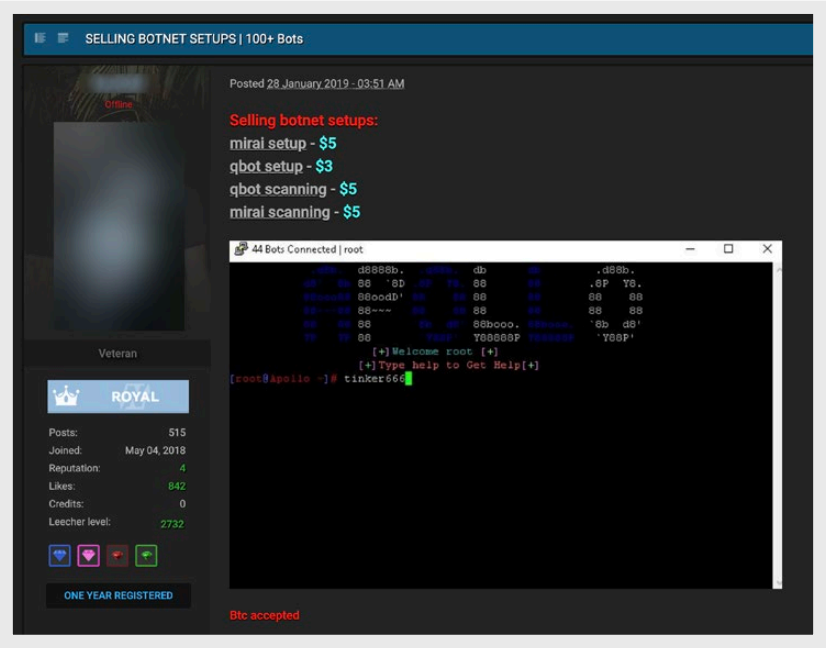


Figure 26. A post selling services to help other criminals set up their own Mirai and Qbot botnets

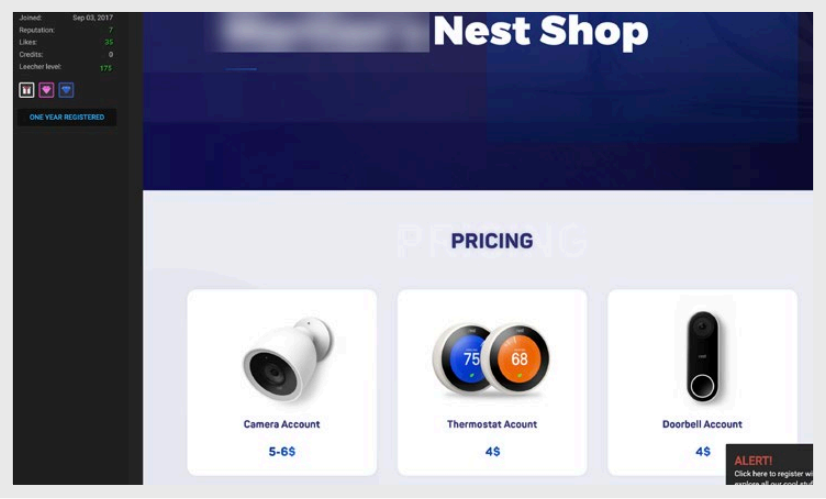


Figure 27. A seller offering webcam access for Nest's outdoor cameras and doorbells

Service	Price
Mirai setup	US$5
Botnet panel/code	US$600
Shodan access	US$25

Table 3. Price of each service found in the English underground forums

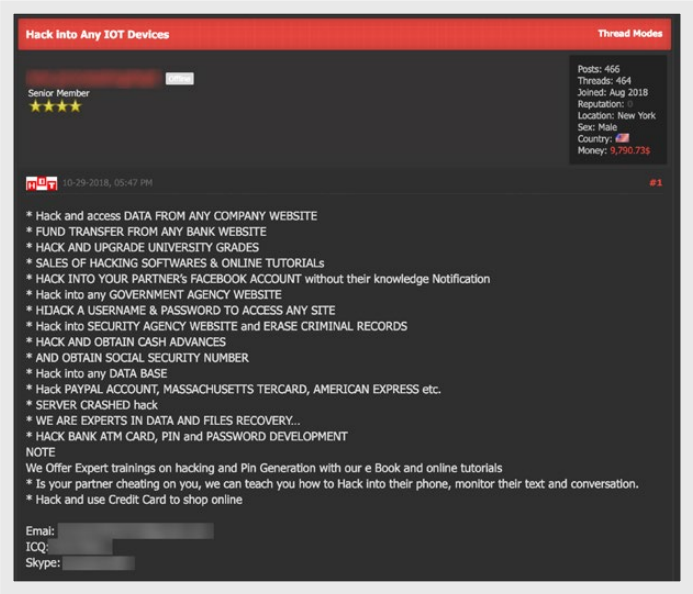


Figure 28. A post offering hacking services specifically for IoT devices

Overall, the English underground has more discussions on information and inquiries than on actual attacks that have materialized and been monetized. Perhaps the most prevalent examples of IoT attacks talked about on English-language hacking forums are Mirai botnet variants.

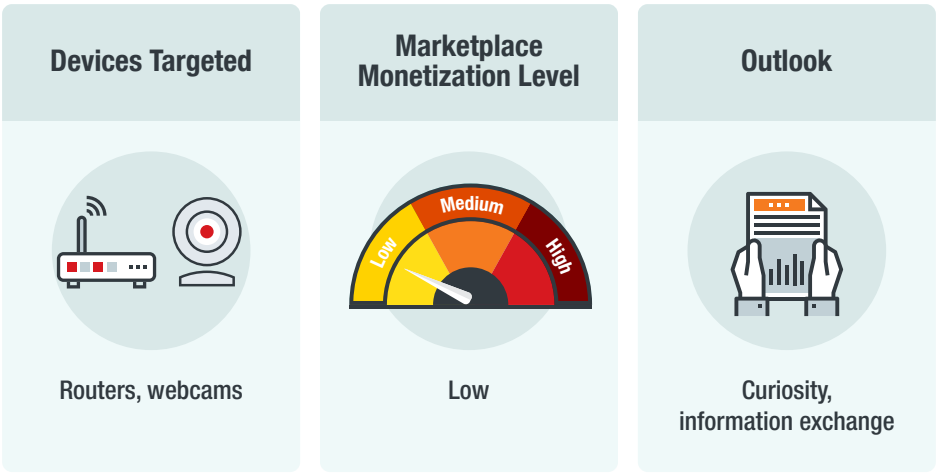
After the router-infecting bot was open-sourced back in 2016, there have been a multitude of modifications to the infamous code that are being shared for free on these forums. The potential for a low-skilled hacker to misuse this information is high, but we have not seen a combined effort from professional criminals to openly monetize this.

What is obvious in hindsight is that the impact of Mirai in the criminal underground has been profound. We summarize its effect into two major items:

- There is now a very small incentive for malware writers to develop new IoT-infecting botnet code. Mirai has become the only code a would-be IoT attacker needs, which in turn stifled the creativity so to speak of cybercriminals in developing original malware. Most “new” IoT botnets today are mere modifications of the Mirai code base.
- Mirai has limited the demand — and therefore the criminal market — for the same kinds of products (i.e., malware). Few criminals are willing to pay for something they can already get for free. Therefore, non-Mirai botnets for sale are uncommon. However, this situation may change if a criminal offers an IoT botnet that has a monetization plan built in. We have not seen this yet, but it’s not an entirely unlikely scenario.

There is one fact about Mirai that should not be overlooked. When talking about this threat, most people will think of large botnets made up of routers. However, a great many new devices coming into the market are Linux-based and they are not limited to routers. This means that the potential for a Mirai botnet operator to automatically infect all kinds of equipment is high and will keep growing as more Linux-based devices are developed and sold.

Arabic Underground Communities



On Arabic-speaking cybercriminal forums, we found entire sections dedicated to technical news and tutorials, where members often discuss recent hacking incidents and how to use upcoming IoT devices. Forum members discuss how Russian hackers are targeting SCADA systems. Hacking webcams and routers have been found in Arabic language forums for years, but there is no mention of these attacks being monetized.

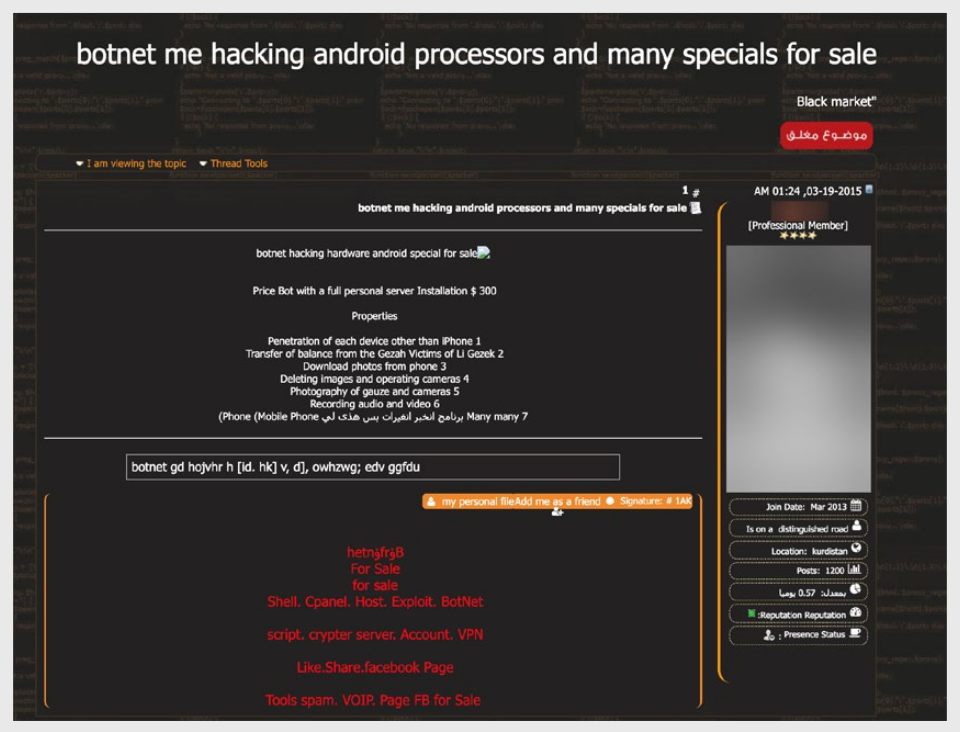


Figure 29. Advertisements for several botnets

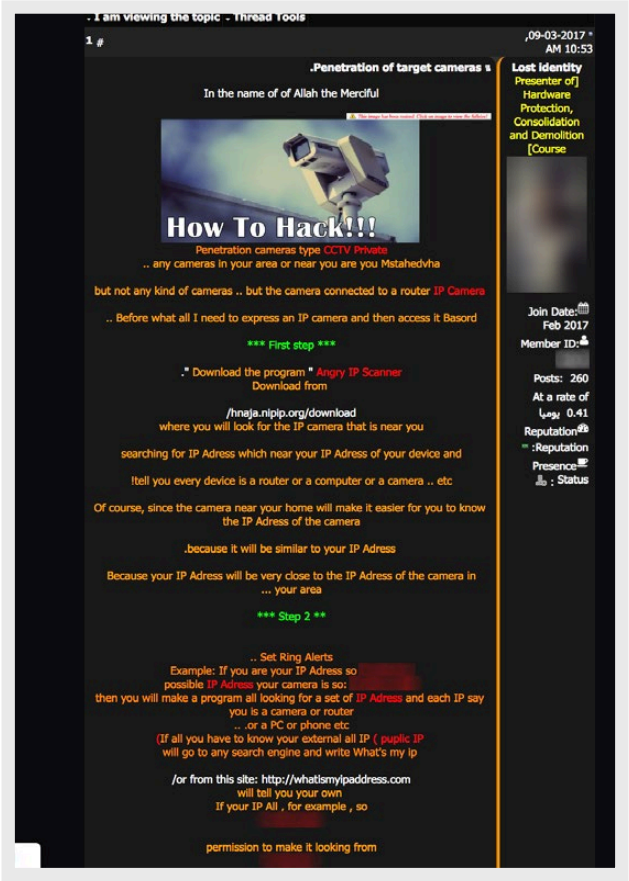


Figure 30. Forum poster sharing a technical article about hacking webcams

Figure 31. Another user sharing an article about hacking webcams

On these forums, we also saw foreign IoT-related news being discussed as a topic of interest. Similarly, we also found users sharing news about recently discovered vulnerabilities and attacks on IoT devices.

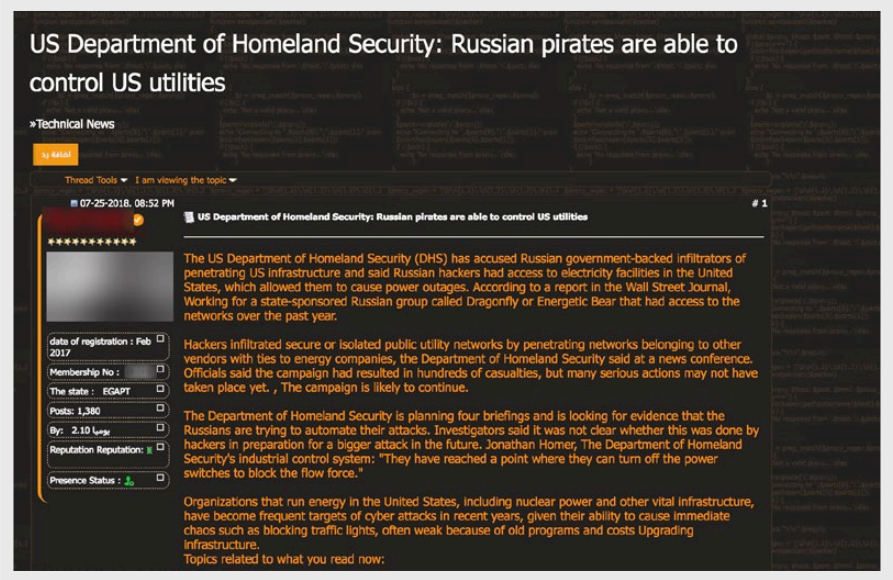


Figure 32. A post sharing an article about how Russian hackers are targeting U.S. SCADA systems

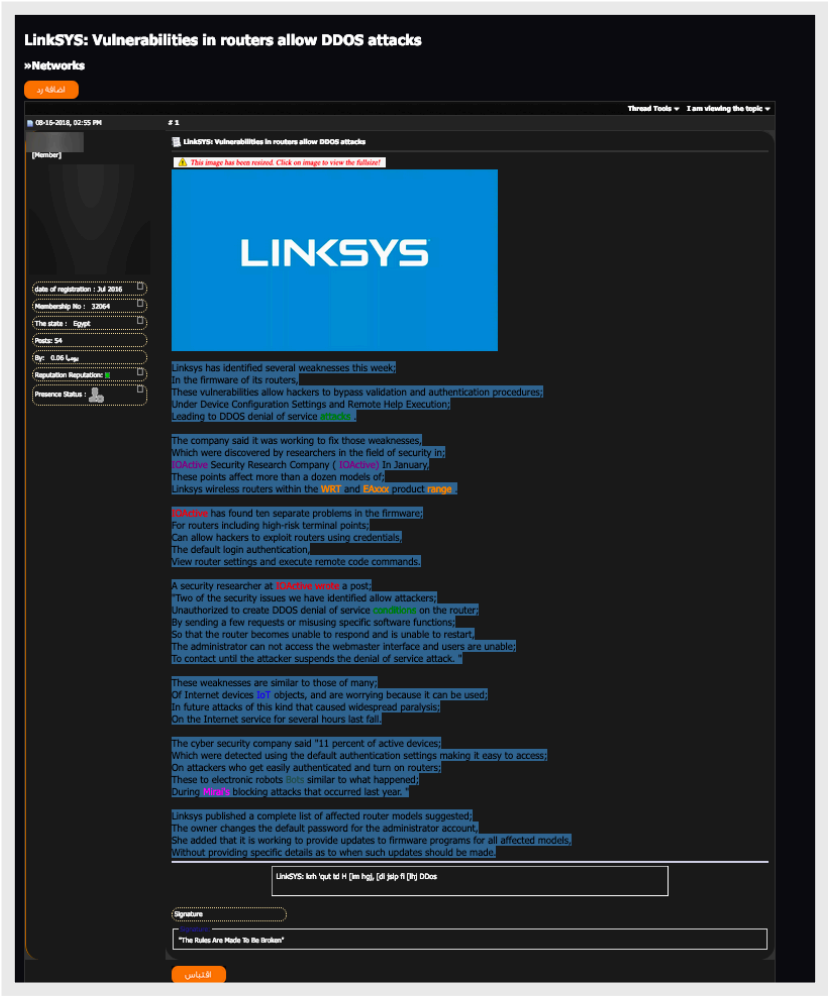


Figure 33. A discussion on a zero-day exploit for Linksys routers

We observed that Shodan is also frequently mentioned and members often ask if there are similar sites for free.

Figure 34. A forum member asking if there are other sites similar to Shodan

In one cybercriminal hacking team forum, we saw free SCADA software available for download. Users can download specific software to study how the systems work.

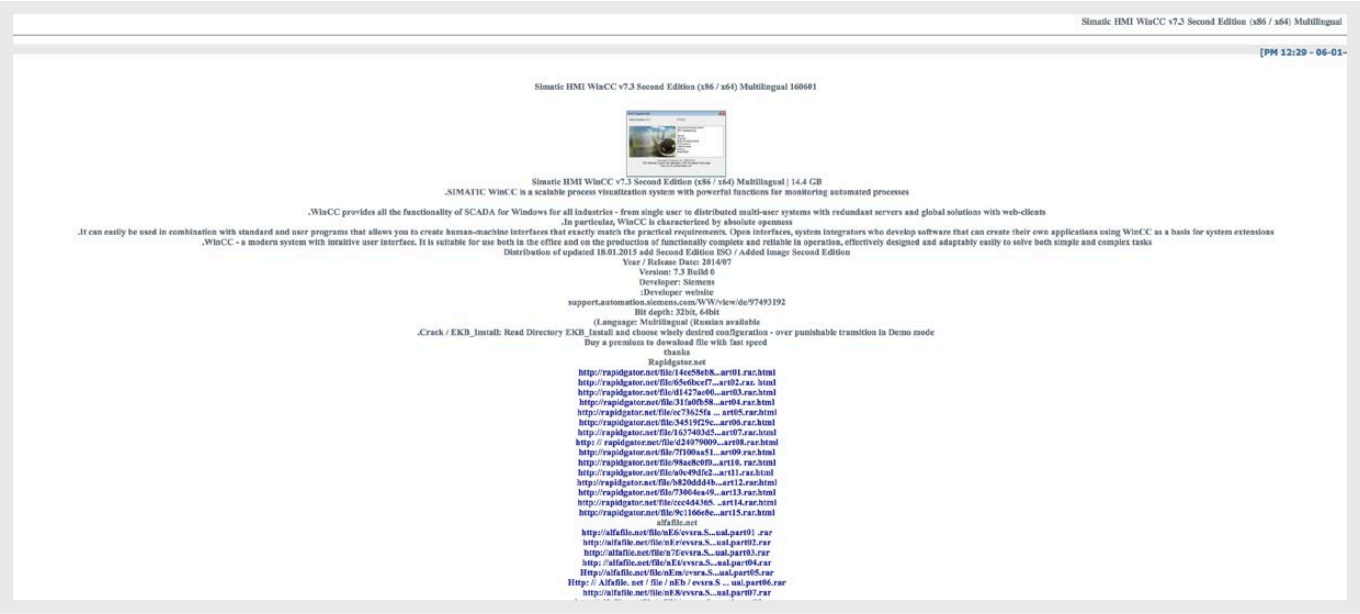


Figure 35. Free Siemens software downloads

The original source code for Mirai and modified versions are shared for free in a similar way to the English underground forums. We also found advertisements looking to purchase bot victims. An example is shown in Figure 36, where the price is provided via private message only. The forum conversation seems to indicate that the seller has access to a large volume of bots consistent with a Mirai-based IoT botnet or similar.

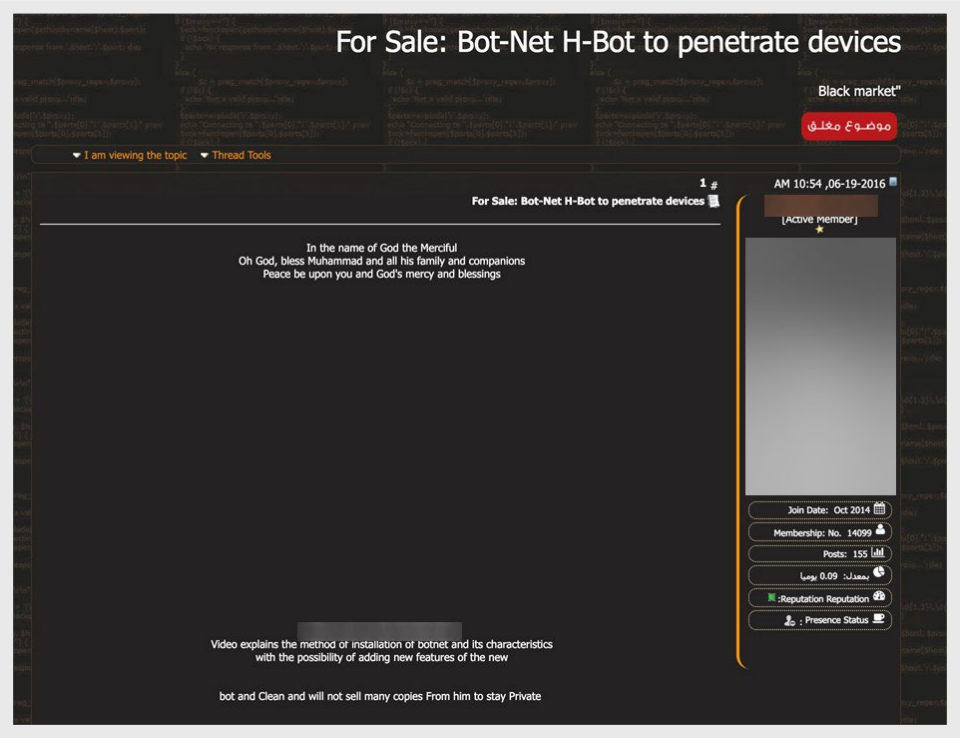


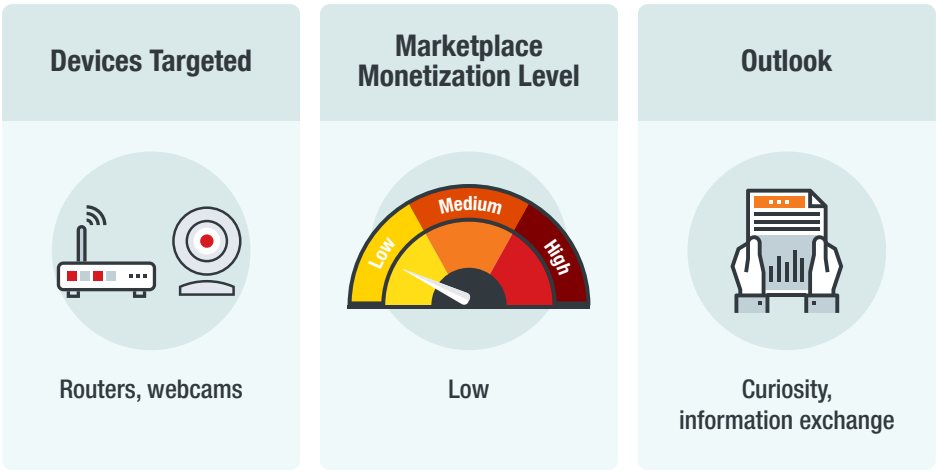
Figure 36. A post showing a botnet for sale

At present, the Arabic cybercriminal IoT market is technically driven and it does not look like they have found a way to monetize any attacks to IoT devices yet. We summarize the services and corresponding prices here, including those that are general network threats.

Service	Price
Mirai	Free
Bot rental (high end)	US$20 per month
Botnet panel/code	US$550

Table 4. Price of each service found in Arabic underground forums

Spanish Underground Communities



On Spanish-speaking cybercrime underground forums, we found plenty of tutorials and discussions on how to exploit devices. Often, they are in the form of articles made by forum users to educate fellow members. For instance, Shodan was discussed on multiple posts in the context of using it to find wireless devices.

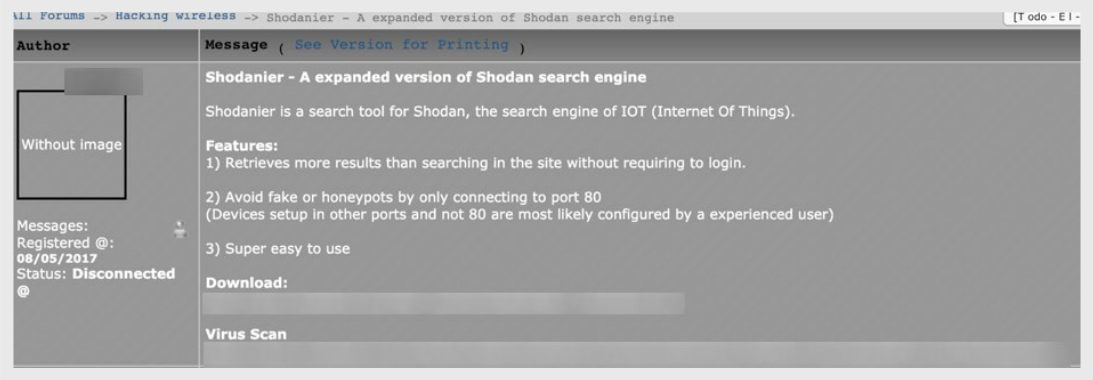


Figure 37. A post discussing how to use Shodan to target wireless devices

On these forums, we have seen research papers on IoT devices being shared and reviewed, including the mentioned paper on a Trend Micro GasPot experiment from 2015.[4] Although less common than routers and webcams, other unconventional devices are sometimes discussed. For instance, we found a post sharing a Google dork to search for unsecured online refrigerators (see Figure 38).

Figure 38. A forum post discussing highlights from Trend Micro's GasPot paper

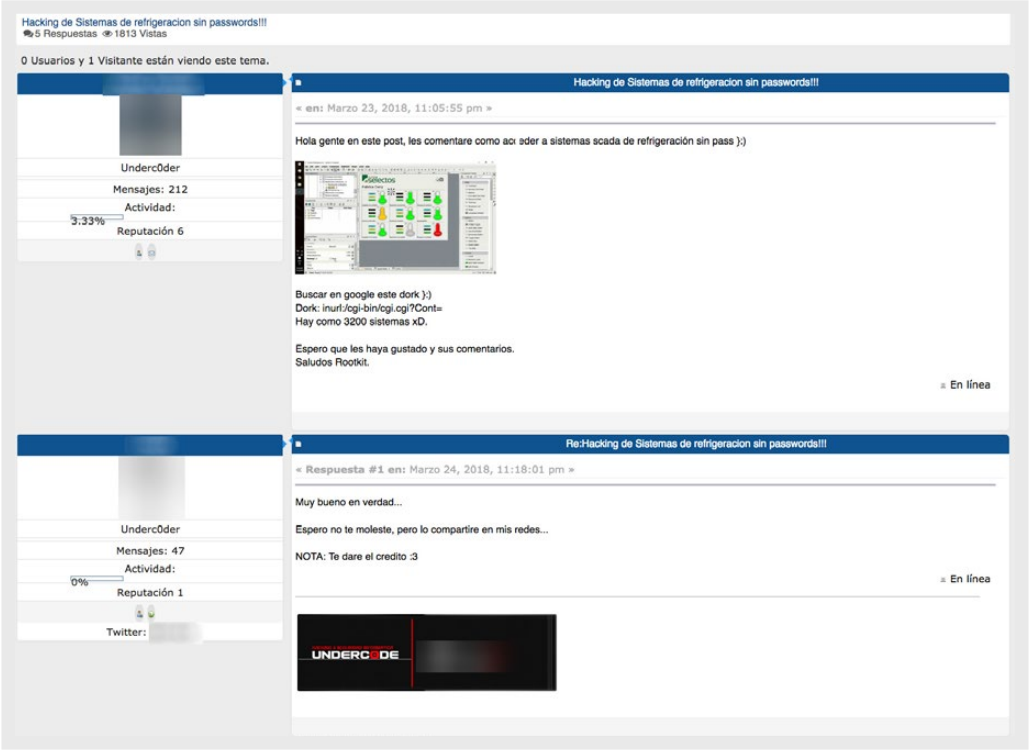


Figure 39. A forum thread showing a Google dork to find unprotected online industrial refrigerators

One of the most interesting discoveries we found was a software called "Simple Active Bot." The same person also offered the software on English forums, but we originally encountered it on a Spanish language site. This software was offered for €1,500. The uploaded sample is designed to target one specific IoT device (in the example in Figure 40, it's TP-Link Archer C5 devices), but the seller claims it supports a few

hundred other kinds of devices. The program uses a canned search on Shodan and shows the results in a simple HTML interface. Supposedly, users of the software can connect to and be authenticated in those devices, allowing them to perform remote tasks. We have not tested the full functionality of the program because there is no trial version of the software available. There's a chance that these claims are entirely false.

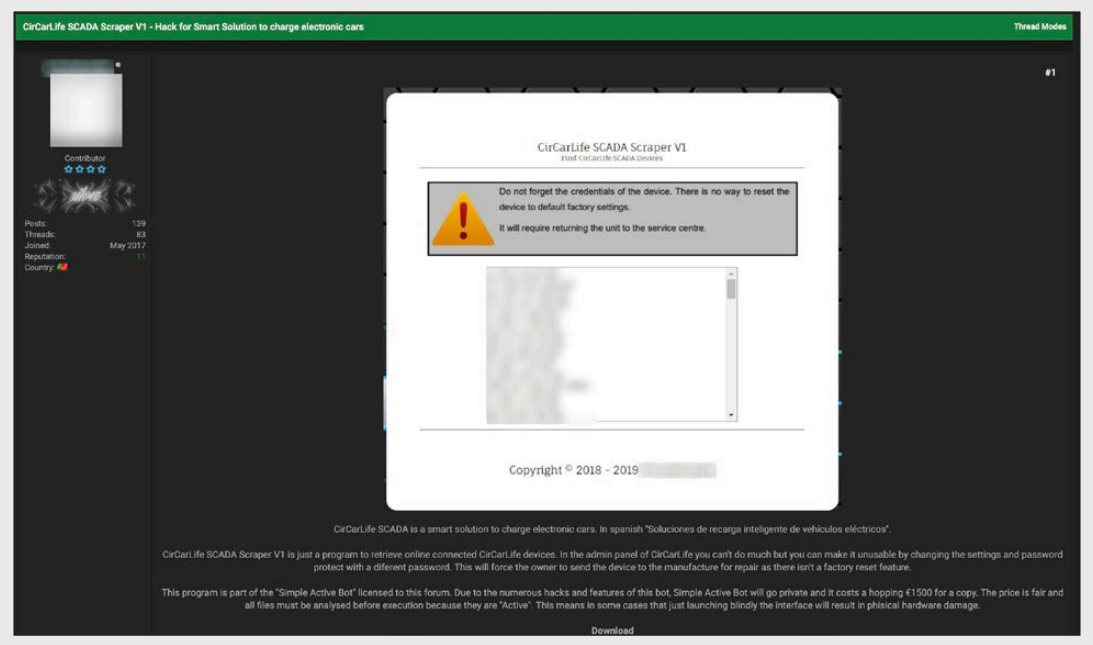


Figure 40. Forum post offering "Simple Active Bot" to automate device discovery using Shodan canned searches

Service	Price
Botnet panel/code	€1,500 (approximately US$1,700)

Table 5. Price of the service found in the Spanish underground forums

The Spanish-language cybercriminal market is also technically driven, with no clear indication that criminals have found a way to monetize IoT attacks. Assuming that the claim of "Simple Active Bot" is real, then it automates the discovery and exploitation of online devices. The way of monetizing those attacks is what is missing. Currently, there is no evidence that criminals on these forums are discussing plans to generate money from such attacks.

Comparative Summary

Figure 41 summarizes the findings for each underground community in terms of topics and also illustrates how these topics are found across several communities. On the left side are the five underground communities; on the right side are the different IoT-related topics discussed in these communities.

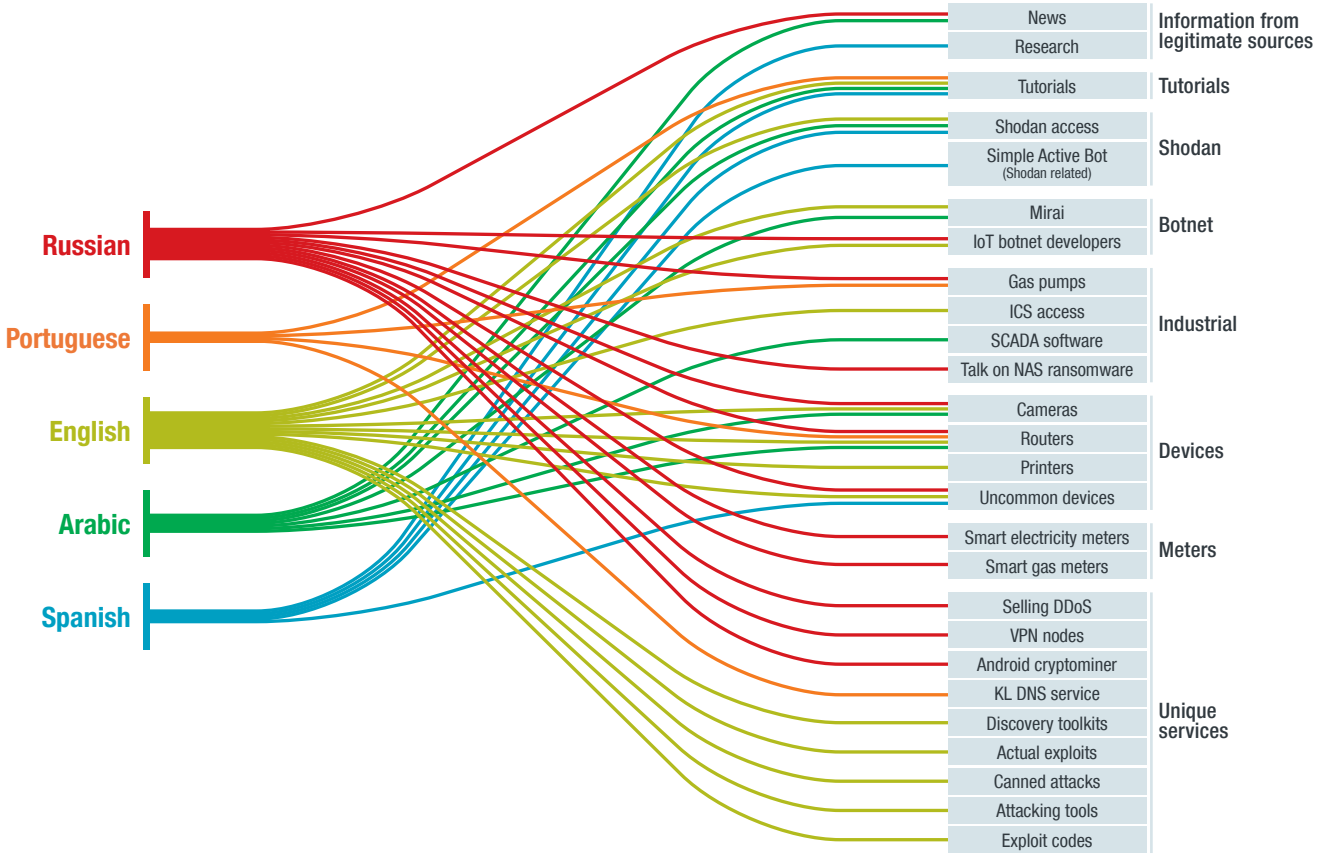


Figure 41. Visual summary of the topics discussed in the five underground communities

Case Studies on IoT Underground Criminals

Before we draw any conclusions, we think it will also be useful to approach the subject of the IoT criminal underground from an attacker's perspective. We picked three threat actors who are currently involved in IoT hacking in one way or another and tracked their hacking careers. This allowed us to see their evolution from plain bad actors to IoT criminals specifically.

One thing we wanted to look at was how a criminal develops a desire to write malware for and hack IoT systems. To do this, we took some of the larger topics and posts that we observed in the underground and started looking into the actors to see if we could find out what drove them to where they are today in the IoT underground. To better understand this, we also wanted to see what financial motivation would drive current and future criminals into conducting IoT attacks.

One of the most prolific cybercriminals thus far whose posts we discussed in the paper is a Brazilian actor who offers a DNS-changing malware targeted at routers (Threat Actor 1). Looking into Threat Actor 1, one can see that he has been around for a while and has changed user handles with few iterations over his criminal career.

Threat Actor 1 started in 2010 by registering domains and a hosting platform. His criminal path didn't begin until 2012, when he started facilitating credit card fraud. We also found that during that year, he was also making fake documents and phishing pages. The forged paperwork included the Brazilian-issued RG and CPF personal IDs, which are documents needed for Brazilian Banking ID Cards. The RG is known as Registro Geral or General Registry[5] while CPF is short for Cadastro de Pessoas Físicas or Natural Persons Register,[6] which is the individual taxpayer's registry. The forged paperwork showed Threat Actor 1's interest in financial crimes, and it escalated in 2013, when he published banking trojans and began selling credit card numbers.

In 2015, he moved on to work on malicious DNS services that would later become the reason why we looked into him. He did not gain much traction on this until more recently. This could be the reason why, aside from the malicious DNS services, he worked on multiple malware attacks and performed bank fraud in 2016. He also dabbled in money laundering around the same time.

In July 2018, Threat Actor 1 finally transitioned to the more modern world of IoT cybercrime. He released a DNS-changing malware (Trend Micro detection name HTML_DNSCHA.SM) along with other malware variants of the same nature. This malware targets multiple types of routers. To do this, he hardcoded default credentials and other commonly used passwords to log into the web admin panels and change the DNS settings using a single HTTP request so that the DNS would be changed to a server under the criminal's control. Threat Actor 1 by then would have access to all requests and can redirect them to high-profile sites such as banking, email services, and any other systems his "customers" may want to pull credentials from. That point is when he really started working on IoT malware to target specific devices though previously he was not leveraging IoT-based attacks at all. This is related to the same attacks that he made involving Brazilian tax cards, but this time, he is working to make financial gains by attacking IoT infrastructure.

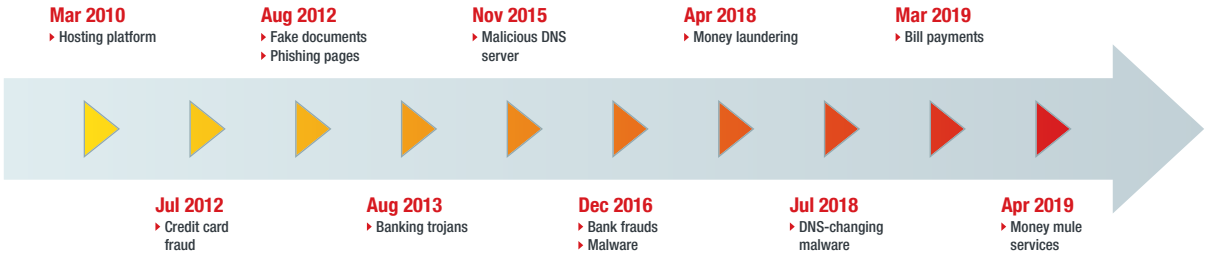


Figure 42. Timeline of the threat actor

Aside from Threat Actor 1, we also followed two other actors that share certain similarities but also have several differences. We looked into an actor from Portugal (Threat Actor 2) that had a similar background that also led him to the criminal underground selling IoT attack tools and services.

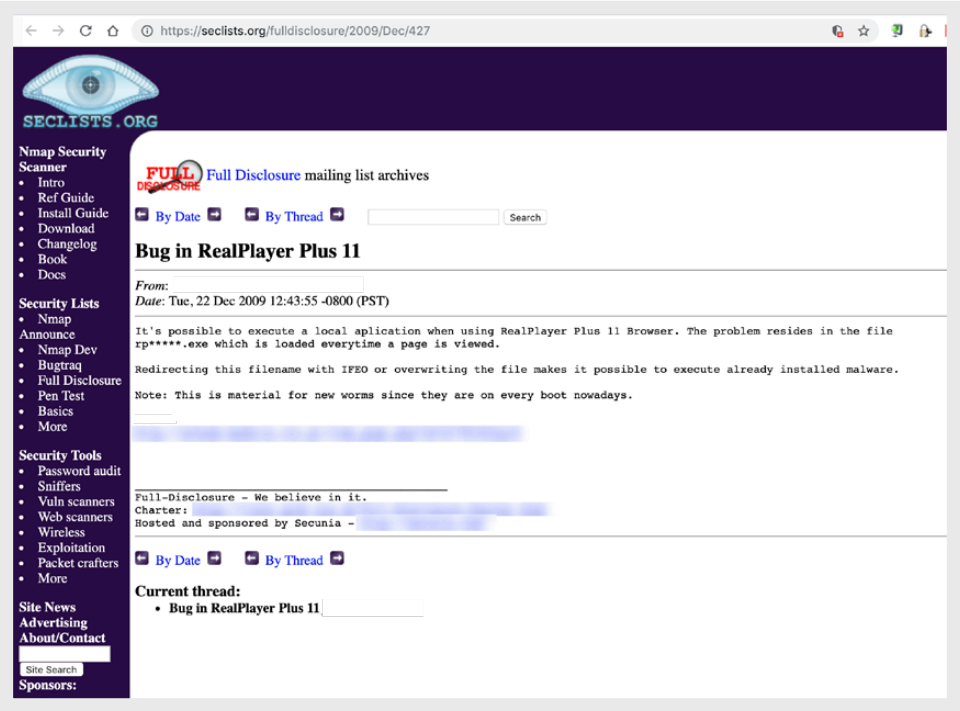


Figure 43. Early activities of Threat Actor 2

In Figure 43, one can see a message in a Full Disclosure mailing list from Threat Actor 2's early days into exploits where he talks about bugs and how to exploit them. Aside from this, he has been very active in a few underground forums over the past decade. Over time, Threat Actor 2 discussed exploits and increasingly moved more to the criminal side and ultimately began creating malware. Threat Actor 2's evolution led him to create the Simple Active Bot IoT tool that we discussed previously in this paper.

Finally, to round things out, we looked at a third actor (Threat Actor 3) that we tracked during this research — one who is likely based in Russia judging from the language, including slang terms, he used. Threat Actor 3 is currently selling VPNs, including SSH, OpenVPN, and Point-to-Point Tunneling Protocol (PPTP), which he claims are implemented on home routers. Unlike other actors, Threat Actor 3 created a new handle — with no previous reputation — to sell access to these systems. The other actors used handles that were either tied to their older handles or used the same email, Jabber, or ICQ, which allowed us to track them over time. For Threat Actor 3, however, we couldn't find anything that linked to his past work. It could be that he is just starting out, or that he is a professional criminal and knows how to start new handles for the products he is trying to sell each time the product advertised changes.

All of these three criminals initially took different paths, from carding, to exploits, to no clear path at all. But all ultimately ended up in the same trade — as early pioneers in the emerging world of IoT cybercrime.

Predictions

Given all the data we have gathered over the course of our research, we predict an evolution of IoT attacks within the next 12 to 18 months. We outline what is seen in the IoT world at present and the corresponding prediction that we think will branch out from them.

1. Routers are the devices that are most frequently attacked. Most of these attacks involve DNS settings modifications. This is relatively easy to prevent. As more internet service providers (ISPs)/ manufacturers start protecting these settings, we are going to see an evolution towards a different kind of router attack.

2. PLCs and the HMIs used to control PLCs are increasingly being found online.[7] Behind these are smart factories or other heavy equipment or machinery. These devices will be attacked more often, to the point where their current policy of "availability first, then security second" will need to shift to a more secure setup. The likeliest business plan to monetize an attack against these devices would probably involve extortion. In this kind of attack, the business model comes from threatening the device's owner with downtime. This way, the criminal can make money out of the attack without the need to understand how the device functions.

3. In the same way that the Mirai botnet has evolved to support more routers and has improved its capabilities, we are bound to see more attacking toolkits that support more devices and are easier to use. We expect to see two major commercial IoT malware kits battle it out to be the most popular. This would be similar to what we saw with banking trojans in the past.

4. More and different kinds of devices are constantly joining the internet as the market for devices becomes more mature.[8] The possibilities for attackers are multiplying, so we can expect to see more advanced threats, like low-level rootkits or firmware infections. New classes of devices that may be susceptible to attack include virtual reality (VR) devices or cryptocurrency mining kits.

5. We have started to see more creative ways of monetizing smart device infections. This tendency will only increase as the ability to attack devices becomes easier and more automated.

6. The increase of mobile connectivity worldwide will allow for faster attacks and additional capabilities for hackers. The switch from 4G to 5G may offer attackers more avenues for exploitation or monetization.[9]

7. Within the next 18 months, we expect to see a much more mature set of attacker business models.

Conclusion

Criminal online communities seem to be very interested in learning how to compromise all kinds of IoT devices. There are many tutorials and research being compiled on hacking techniques, vulnerability exploitation, and even source code for script kiddies and any curious individual to do plenty of damage. We have not yet seen signs of any concerted effort on the part of criminal groups to massively damage or compromise any IoT infrastructure. Any mass infection we have seen are usually caused by an exploitable vulnerability — as in the MikroTik case from Brazil — and by weak credentials — as in every Mirai attack. We are starting to see the first attempts to find ways to monetize device infections and these may boost IoT attacks.

Additionally, we would like to mention that nation-states and more dangerous threat actors are also infecting IoT devices to use them as DoS platforms and proxy agents. We have not touched on these attacks since they fall out of the scope of this paper. Nevertheless, criminals are also finding a similar use for infected devices, as we outlined in the previous sections, and this goes to show that those advanced attack scenarios are possibly what "worse" looks like in this domain.

Bigger and juicier targets, such as critical infrastructures,[10] are of course subject to attacks, but those are more likely to be very targeted in nature rather than more widespread criminal attacks. Cybercriminals are inherently motivated by financial gain and, so far, there are only a few ways of getting money from IoT attacks. The bad news: Criminals are refining their business models to include these online devices and, although limited, they are finding a certain measure of success.

We surmise that this trend will continue. As more devices with better capabilities connect to the internet, cybercriminals will keep trying to find new ways of infecting them and make money from those infections.

Defending Against IoT Attacks

Those who have a stake in the IoT should not wait for threat actors to find a way to monetize attacks against it. Knowing that different cybercrime underground communities already contain extensive conversations on different IoT device weaknesses and attack opportunities should be enough of an impetus to reevaluate current defenses.

For manufacturers, implementing security from the design phase can help reduce the number of openings found by cybercriminals in numerous devices streaming into the market. Trend Micro IoT Security provides network and edge layer protection for IoT device-makers to integrate with IoT devices, mobile apps, web apps, and IoT gateways.

Integrators and end users, on the other hand, should remain vigilant in choosing the devices that they put online. Users are responsible for implementing secure configuration and setup of their IoT devices to reduce the risk of these very devices being used for illicit means. For integrators, having complete visibility over each device connected to a single network is crucial in gaining control not just over the IoT environment itself but also over the threats and weaknesses each device might bring to the entire network.

Employing cybersecurity solutions can be an option for users to gain better visibility and control over connected devices. Users can consider, for example, the Trend Micro™ Home Network Security tool,[11] which can provide both visibility and protection for all connected devices inside the home, while organizations can opt for the Trend Micro Deep Security™ solution, which offers security for physical, virtual, cloud, and hybrid environments.

References

1. Trend Micro Forward-Looking Threat Research Team. (8 May 2018). *Trend Micro*. "Exposed Video Streams: How Hackers Abuse Surveillance Cameras." Last accessed on 30 July 2019 at https://www.trendmicro.com/vinfo/ie/security/news/internet-of-things/exposed-video-streams-how-hackers-abuse-surveillance-cameras.

2. Trend Micro. (3 August 2018). *Trend Micro*. "Over 200,000 MikroTik Routers Compromised in Cryptojacking Campaign." Last accessed on 30 July 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/over-200-000-mikrotik-routers-compromised-in-cryptojacking-campaign.

3. Kyle Wilhoit and Stephen Hilt. (5 August 2015). *Trend Micro*. "The Gaspot Experiment: How Gas-Tank-Monitoring Systems Could Make Perfect Targets for Attackers." Last accessed on 1 August 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-gaspot-experiment.

4. Kyle Wilhoit and Stephen Hilt. (5 August 2015). *Trend Micro*. "The Gaspot Experiment: How Gas-Tank-Monitoring Systems Could Make Perfect Targets for Attackers." Last accessed on 1 August 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-gaspot-experiment.

5. Fundação Nacional do Índio – FUNAI. (n.d.). *FUNAI*. "Carteira de Identidade – RG (Identity Card – RG)." Last accessed on 5 August 2019 at http://www.funai.gov.br/index.php/docb/carteira-de-identidade-rg.

6. Fundação Nacional do Índio – FUNAI. (n.d.). *FUNAI*. "Cadastro de Pessoa Física – CPF (Cadastro de Pessoa Física – CPF)." Last accessed on 5 August 2019 at http://www.funai.gov.br/index.php/docb/cadastro-de-pessoa-fisica-cpf.

7. Matsukawa Bakuei, Ryan Flores, Vladimir Kropotov, and Fyodor Yarochkin. (3 Apr 2019). *Trend Micro*. "Securing Smart Factories: Threats to Manufacturing Environments in the Era of Industry 4.0." Last accessed on 5 August 2019 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/security-in-the-era-of-industry-4-dealing-with-threats-to-smart-manufacturing-environments.

8. Dan Goodin. (5 Aug 2019). *Ars Technica*. "Microsoft catches Russian state hackers using IoT devices to breach networks." Last accessed on 6 August 2019 at https://arstechnica.com/information-technology/2019/08/microsoft-catches-russian-state-hackers-using-iot-devices-to-breach-networks.

9. Trend Micro Research and Europol's European Cybercrime Centre (EC3). (21 Mar 2019). *Trend Micro*. "Cyber-Telecom Crime Report 2019." Last accessed on 6 August 2019 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/global-telecom-crime-undermining-internet-security-cyber-telecom-crime-report.

10. Stephen Hilt, Numaan Huq, Vladimir Kropotov, Robert McArdle, Cedric Pernet, and Roel Reyes. (30 October 2018). *Trend Micro*. "Critical Infrastructures Exposed and at Risk: Energy and Water Industries." Last accessed on 5 August 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exposed-and-vulnerable-critical-infrastructure-the-water-energy-industries.

11. Trend Micro. (n.d.). *Trend Micro*. "Home Network Security." Last accessed on 5 August 2019 at https://www.trendmicro.com/en_au/forHome/products/homenetworksecurity.html.

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 threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

TREND MICRO™ | research