

2015
**Highlights &
Trends in the
Deep & Dark Web**

February 2016

Contents

Click on a title to navigate to the page

1. Executive Summary	1
2. Dark Net Markets in Transition	
Background	2
Dark Net Market Risks and Increased Security	2
Drugs and Fraud Products Are Big	3
Cross Pollination	4
Conclusion	4
3. Fraud – Account Takeover Landscape	
Background	5
Infection of Client Computers	5
Bruteforcing Account Credentials	6
Conclusion	7
4. Fraud - Cashout and Crowdfunding	
Background	8
Cashout	8
Crowdfunding	9
Conclusion	9
5. New Notable Malware-as-a-Service Offerings	
Background	10
Overflow Bot	10
Ganjaman Android Malware	11
AlphaLeon	12
Turnkey Ransomware	13
Conclusion	13
6. Chinese Cybercrime – The Trend Towards Internationalization	
Background	14
Branching Out Internationally	14
The Domestic Approach	15
Conclusion	16
7. The French Underground – Managing Increased Media Visibility	
Background	17
Increased Media Coverage	18
Measures to Deter Undesirables	18
Conclusion	19
8. Hacktivists and Chaotic Actors	
Background	20
Doxing Is Becoming Popular	20
Awareness of Swatting Is Increasing	21

8. Hacktivists and Chaotic Actors (cont'd)	
DDoS Is Getting Worse	21
Chaotic Attacks Continue to be Fueled by the Media	21
Conclusion	22
9. Jihadi Underground Forums – Shifting Alliances	
Background	23
Shifting Towards ISIS	23
Technically Savvy Jihadists	24
Conclusion	25
10. The “Crypto-Wars” and Tor Hidden Services	
Background	26
The Encryption and Backdoor Debate	26
Dark Web Density	26
.onion Survey	27
Conclusion	28
11. Final Conclusion	29
Learn More	30

Executive Summary

2015 was a year of escalating activity in the Deep & Dark Web. Illicit goods marketplaces matured and new, specialized marketplaces emerged. Novel schemes for fraud and financial cybercrime appeared, as did offerings, and business models allowed a larger class of less sophisticated actors to engage in cybercrime.

Discussions about encryption and privacy entered the political domain while increasing numbers of hacktivists and chaotic actors looked for personal fame and attention instead of political gain. The Deep & Dark Web has been, by nature, an international phenomenon, and 2015 brought a number of new and telling trends in Europe, the Middle East, and Asia, including the maturing of the Chinese and French underground communities.

Organizations are becoming aware of the value of staying one step ahead of cyber and physical threats with intelligence from the Deep & Dark Web that provides context and an enhanced understanding of risks and exposure. Tactical, operational, and strategic intelligence reduces costs from fraud, data loss, and reputational damage and provides insight into potential criminal or terrorist activities that could affect the organization's business, employees, partners, and customers. Flashpoint subject matter experts constantly monitor Deep & Dark Web activity to extract intelligence and context. As we begin the new year, these subject matter experts compiled a list of what they've observed as the top highlights and trends of the past year. This whitepaper contains their thoughts and insights into highlights and trends of 2015.

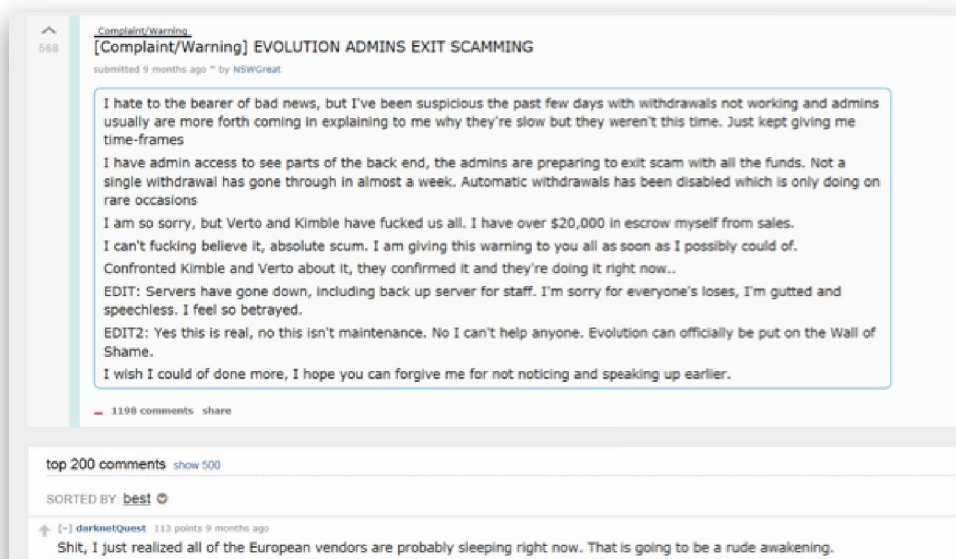
Dark Net Markets in Transition

Background

In 2015, the illicit marketplaces hosted in the Dark Web and accessible via the Tor network, also known as Dark Net Markets (DNMs), have seen a renewed focus on security, professionalization of the markets, and minimizing points of transaction requiring good faith. There has also been a strong trend towards increasing sales of narcotics as lethal products fall off. Site-on-site cyberwars have increased as the DNMs continued to compete for market share. Finally, Flashpoint subject matter experts are also observing a cross-pollination between DNMs and the cybercrime community.

Dark Net Market Risks and Increased Security

The prosecution of Silk Road vendors and owners by federal courts revealed law enforcement to be more capable of penetrating cryptocurrencies and hidden services than the community expected. The Evolution market, one of the largest in the space, conducted an exit scam which stole over \$12 million from customers, prompting a wave of paranoia and point-of-sale reform. This skittishness has only been reinforced on other DNMs, with two false alarms about Nucleus exit scams, a BlackBank exit scam, and fears of AlphaBay following the same playbook.



Confirmation of Evolution Exit Scam

For fear of attracting close scrutiny from law enforcement, Agora market, one of the oldest, largest, and most reliable DNMs, officially forbade the sale of lethal implements on its site. Agora shortly thereafter announced that it was closing operations for the foreseeable future, only reinforcing the popular perception that the store had been compromised. After that precedent, weapons sales fell dramatically across all markets, and no new market has been willing to host the open sale of weapons.

The combination of the Evolution exit scam and Silk Road criminal convictions have caused DNM owners to place renewed emphasis on security and offering technical means to reduce customer and vendor steps which require implicit trust. Multi-signature verification has gone from the cutting edge to the expected norm for any major market, and there is a push to create escrow systems which are independent of the market owners, clients, and vendors, though that system is yet to be implemented.

Drugs and Fraud Products Are Big

Within the DNM communities 2015 was the year of the online drug market. Following the busts of the initial Silk Road and Silk Road 2.0, several new markets have sprung up to take their place with an increasing proliferation of narcotics. In the top three markets alone, there are over 25,000 listings for narcotics on a given day, ranging from illegal prescriptions and marijuana to pure cocaine. Most of these are in small, personally consumable quantities, though there are a few exceptions in sizes that would allow for resale at the point of delivery. Additionally, nearly 50% of the minor markets and “vendor shops” specialize solely in narcotics distribution, and of the remaining minor markets, all but three dedicated cryptography/hacker markets have more narcotics listings than any other category.

BROWSE CATEGORIES	
▶ <input type="checkbox"/> Fraud	11678
▶ <input type="checkbox"/> Drugs & Chemicals	44896
▶ <input type="checkbox"/> Guides & Tutorials	5136
▶ <input type="checkbox"/> Counterfeit Items	2147
▶ <input type="checkbox"/> Digital Products	4656
▶ <input type="checkbox"/> Jewels & Gold	630
▶ <input type="checkbox"/> Weapons	696
▶ <input type="checkbox"/> Carded Items	1157
▶ <input type="checkbox"/> Services	2565
▶ <input type="checkbox"/> Other Listings	976
▶ <input type="checkbox"/> Software & Malware	631
▶ <input type="checkbox"/> Security & Hosting	208

AlphaBay Product Categories

After drugs, fraud products, a mix of stolen credit cards, documents, and accounts,

are the second most available goods on the major markets. AlphaBay in particular has gained significant tractions as the DNM of choice for fraud and cyber crimeware products. Launched following the closure of the Tor Carding Forums (TCF) in December 2014 by one the TCF moderators Alpha02, AlphaBay has continued promoting itself on the Russian open web cybercrime forums like Monopoly and Vor.

**alpha02 says:**

All tutorials (quality ones, not burnt, and those who make sense) have been imported to AlphaBay Market. AlphaBay will have the same sections than TCF and will seek to fill the void left by TCF closure.

Verto's work will not be forgotten, and all fraud forums will move to AlphaBay.

Cleartnet landing: <http://alphabay.me>

Onion link: <http://pwoah7foa6au2pul.onion>

See you there!

© 12/21/2014 6:14 p.m.

AlphaBay Announced on Tor Carding Forums

Cross Pollination

Following the initial skepticism about DNMs from members of traditional cybercrime forums, 2015 has seen a significant cross-pollination of membership between the two types of communities. Evidencing this trend are new accounts on DNMs registered under the same aliases in both communities, both by vendors and consumers of illicit products and services. Flashpoint expects to see continued interest from the Deep Web forum members in DNMs, but traditional cybercriminal forums and Dark Net Markets will retain their unique identities for the foreseeable future.

Conclusion

The DNMs are a protean piece of the Deep & Dark Web. As buyers and vendors perceive new risks, the DNMs evolve to provide new security measures. The DNMs also adapt in response to outside influence, such as additional scrutiny from law enforcement. Currently, DNMs focus on drugs and fraud products, and the expectation is that this will continue for the foreseeable future.

Fraud – Account Takeover Landscape

Background

Account takeover fraud represents the major source of income for financially motivated cybercriminals. Therefore, a large percentage of malicious activity on the Deep & Dark Web supports a single objective: to steal authentication credentials. These credentials may range from logins, passwords, and device IDs, to answers to security questions, or one-time tokens. In 2015, Flashpoint subject matter experts observed a new generation of underground marketplaces. Proprietors behind these so-called “account shops” are increasingly acting as brokers between cybercriminals who compromise credentials for financial services, retail, and other online portals, and other cybercriminals leveraging the credentials for profit.

The tactics used by suppliers of compromised credentials consist of two broad categories: infection of client computers (also known as accounts from logs), and bruteforcing.

Infection of Client Computers

Suppliers of compromised accounts exfiltrate victim activity logs from the infected machines, parse them for credentials, and commission the digital goods to proprietors of underground marketplaces.

An example of this trend is the nascent “Account Shop” marketplace. Its proprietors purchase spent logs in bulk, parse them for credential pairs, and lists the results on their website. Launched in July 2015 as a Tor website, the marketplace currently lists for sale online credentials for 110 US banks and credit unions, a range of online payment systems, and large retailers.

Credentials for organizations in the following categories are available for purchase from “Account Shop”: US Banks, EU Banks, Canadian Banks, Credit Card Accounts, US Internet Brokers, Retailers, Employer accounts (Monster and Indeed), Cell Phone Providers, Online Payment Systems, Frequent Flyer Accounts, and Others.

Банки US	Банки Европы	Банки Австралии	Банки Канады	Accounts With Card Info(Enroll)	Интернет Брокеры USA
Магазины	Аккаунты Работодателей	Сотовые операторы	Платёжные системы	Аккаунты Авиакомпаний	Прочее

Categories of Accounts

The seller takes care to describe precisely what information will be available with each purchase to avoid future disputes with unsatisfied customers with statements such as:

- Amazon accounts, includes additional data like the credit card number
- Enrolled Wells Fargo credit card accounts, includes additional information like the full card number, cvv, etc. Some come with email access.
- Verizon accounts, collected from web-inject logs that include answer to secret questions. Some are from plain logs. All accounts were checked with our own checker.

The screenshot below illustrates the availability of credentials for some of the affected organizations and suggests that no community bank is too small to be targeted.

Given the exuberant reviews received since its launch, the “Account Shop” marketplace can be expected to continue attracting both new customers and suppliers of botnet logs as it builds momentum. Assuming the business model proves viable, it is likely that other players will enter the market, providing technically unskilled fraudsters with an increasingly wide range of income opportunities.

 1ststatebank.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.	 communitychoicecreditunion.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.	 fnb.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.
 fbandt.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.	 keybank.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.	 abcfcu.org Доступ к аккаунтам без доступа к money. Все отмены в наложении.
 irland.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.	 midwest.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.	 nasb.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.
 peoples.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.	 campusfederal.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.	 snofalls.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.
 starchoice.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.	 piedmontbank.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.	 spartan.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.
 suffolk.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.	 tellico.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.	 tara.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.
 pvnb.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.	 genfed.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.	 washstate.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.
 community.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.	 farmers.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.	 idaho-central.com Доступ к аккаунтам без доступа к money. Все отмены в наложении.

Stolen Online Banking Credentials

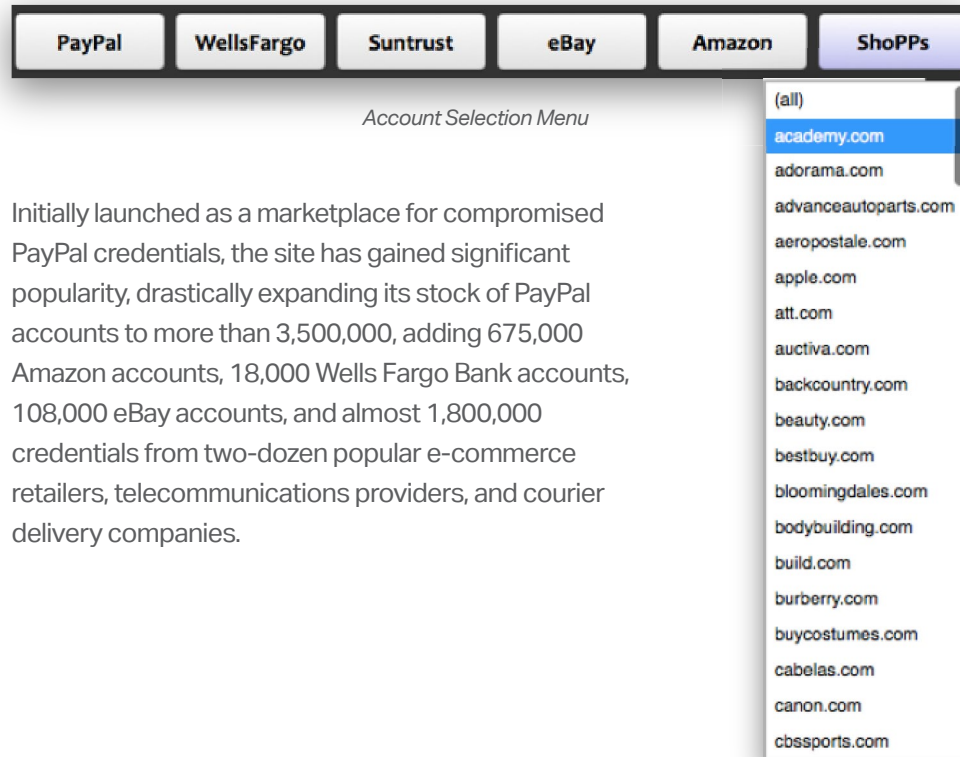
Bruteforcing Account Credentials

Another major source of compromised account credentials is password reuse. Email and password pairs found on the various paste sites or purchased from other hackers are used in attempts to log into a series of online portals.

Owners of bruteforcing tools claim success rates of 5-10%. In other words, every 10th to 20th pair can be expected to provide access to popular online portals like PayPal.

The proprietors of one account marketplace have listed over 1.6 million usernames and password pairs across dozens of affected organizations.

Besides the popular credentials for organizations shown above, the “ShoPPs” button brings up the list of e-commerce websites, for many of which there are thousands of credentials.



The screenshot shows a horizontal menu with six buttons: PayPal, WellsFargo, Suntrust, eBay, Amazon, and ShoPPs. Below the buttons is the text "Account Selection Menu". A dropdown menu is open under the ShoPPs button, listing various e-commerce websites. The list includes: (all), academy.com, adorama.com, advanceautoparts.com, aeropostale.com, apple.com, att.com, auctiva.com, backcountry.com, beauty.com, bestbuy.com, bloomingdales.com, bodybuilding.com, build.com, burberry.com, buycostumes.com, cabelas.com, canon.com, and cbssports.com.

Initially launched as a marketplace for compromised PayPal credentials, the site has gained significant popularity, drastically expanding its stock of PayPal accounts to more than 3,500,000, adding 675,000 Amazon accounts, 18,000 Wells Fargo Bank accounts, 108,000 eBay accounts, and almost 1,800,000 credentials from two-dozen popular e-commerce retailers, telecommunications providers, and courier delivery companies.

Conclusion

The success of marketplaces that specialize in account takeover fraud will enable a wider range of fraudsters to more easily execute fraud schemes to generate income.

Fraud - Cashout and Crowdfunding

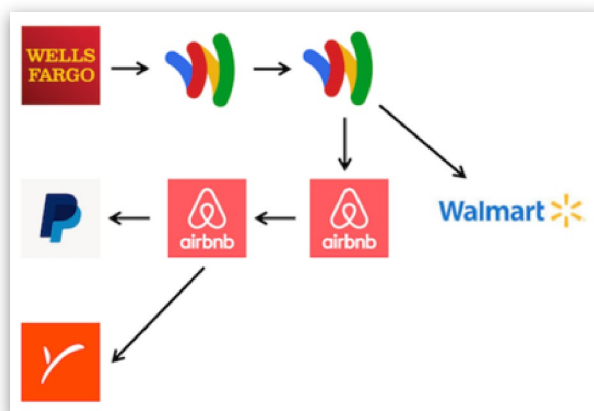
Background

With the rapid evolution of the cybercrime industry and the proliferation of communities in the Deep & Dark Web, offering easy access to an abundant supply of stolen financial information, personally identifiable information (PII), and cybercrime tutorials, the barrier of entry to the world of cyber crime has never been lower. While account takeover is responsible for most of the malicious activity, Flashpoint subject matter experts observed that successful account compromise is only the first step in the chain of transactions that leads to cash. 2015 was marked by further evolution of common cashout tactics, as well as the introduction of several novel schemes. The emergence of new peer-to-peer payment transmission services has provided fraudsters with an array of tools for funneling stolen funds.

Cashout

In one novel method shared on a cyber fraud forum, a user described a successful cashout chain that involved sending "gifts" to fake recipient accounts on Tindr, or "donations" on the fundraising platform PayItSquare, all of which were funded with compromised bank accounts of credit cards.

A clever variation on the traditional money laundering chain was shared by a fraudster in an attempt to boost his reputation on a criminal forum. The movement of funds from compromised bank accounts in a multi-step cash out loop involved registration of new sending and receiving Google Wallets. Funds flow from compromised bank accounts, to the sending Google Wallet, to the recipient Google Wallet. From there, the funds are tumbled once again through sending and receiving Airbnb accounts, before getting converted to a currency equivalent in PayPal or Payoneer. Finally, the funds are cashed out by purchasing gift cards from a variety of ecommerce stores, among them Rakuten, Walmart, Gyft, and Overstock.



Personally identifiable information (PII) such as Social Security Number and date of birth required for Google Wallet verification is available on several underground marketplaces for as low as \$3.00. To complete phone verification, a Google Voice or other VoIP number is often used.

Crowdfunding

Crowdfunding campaigns are another relatively low-tech means by which fraudsters can launder stolen funds, or simply scam individual investors. In 2015, a group of fraudsters connected through a cybercrime forum launched a crowdfunding campaign for a vaporware smartphone.



With over \$120,000 in initial funding, the group developed a spiffy prototype, showcasing the device on their website. During some six months of preparation, promotional videos were filmed, the corporation was registered in Hong Kong, and a heavy marketing campaign began. Within days, influential tech blogs noticed the upstart company, which was

promising to deliver an extremely powerful smartphone at very competitive pricing. In short order, pre-orders from eager customers poured in, eventually reaching over \$750,000 in sales—surpassing the expectations of the fraudsters.

Conclusion

Fraudsters will continue to exploit Internet payment systems and the public's increasing trust in business conducted on-line to develop and execute defrauding schemes.

New Notable Malware-as-a-Service Offerings

Background

Malware-as-a-service has remained a significant part of the thriving marketplace of illicit products offered for lease or sale on Russian-language cybercriminal forums in the Deep & Dark Web. While many malware developers prefer steady work supporting “private projects” such as Dyre and Cryptowall, some have continued building their brands as reliable producers of malware or related services. Flashpoint subject matter experts have observed several actors active on Russian underground forums who succeeded in developing reputable services in 2015. Below are a couple of examples.

Overflow Bot

In November 2015, an advertisement for a powerful new DDoS bot was posted on a Russian cybercrime forum. The bot’s developer “Sosweet” is a provider of bulletproof hosting services through a server farm in Ukraine. Unlike a traditional bot, Overflow botnet typically consists of 2 to 5 Linux servers with high-bandwidth uplinks through Sosweet’s own data center.

The bot offers a range of powerful and advanced attack options, including amplification attacks that leverage SSDP, DNS, TCP, and NTP reflection. The bot has a built-in scanner that continuously updates its database of devices that may be used in reflection attacks.

One of the bot’s most salient purported features is the ability to stage attacks that penetrate Cloudflare DDoS protection. Overflow received a positive review from “Ar3s,” one of the most authoritative members of the Russian cybercriminal underground, who wrote that he was able to take down his own forum, with only three Linux bots.

The bot’s designers claim that the botnet offers a number of advantages over competitors, including full bypass of VAC or Voxility protections, as well as implementation of the latest attack vectors.

Ganjaman Android Malware

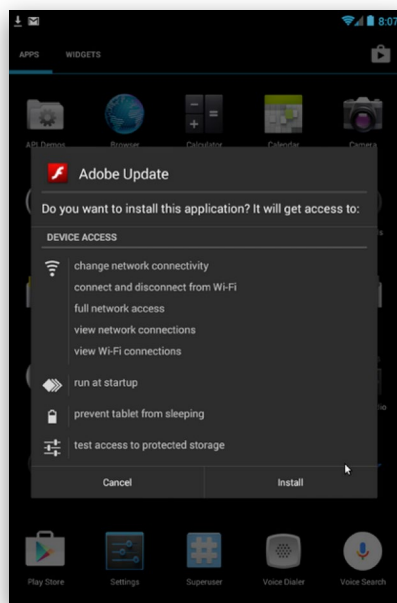
As users increasingly turn to their mobile devices to conduct financial transactions, porous security of Android devices makes mobile malware-as-a-service an attractive proposition for cybercriminals. 2015 saw the continued proliferation of services around the monetization of access to infected Android devices. These products have expanded beyond the creation and distribution of malicious APK files to crypting, socially engineered installation landing pages, and compromised developer Google Play accounts, among others.

"Ganjaman" is a prolific author of malware specializing in the development of Android bots. In February 2015, Ganjaman released a product entitled "GM Bot," which he dubbed "Today's Leading Android Malware." Besides the collection of credit cards and personally identifiable information (PII), GM Bot includes the ability to integrate HTML injects. A unique feature of the bot is its ability to lock up the Android device until the desired data is entered. In September Ganjaman updated the malware by adding the capability to capture incoming text messages, send out messages, and forward calls.

In March, Ganjaman released "Skunk," a malware that promises to steal credentials from Android banking applications by injecting JavaScript code into running banking apps. A feature shared with GM Bot is the ability to place voice calls and send text messages through the infected phone. The most innovative feature is the ability to load HTML/JavaScript code from the administrative panel, allowing up to 50 different preconfigured designs for banking apps. Skunk's admin panel facilitates the interception of SMS messages, apps, and contacts from the infected phone, as well as the complete lock or reset of the infected device.

Ganjaman subsequently offered for sale injects for dozens of banks around the world developed specially for Skunk.

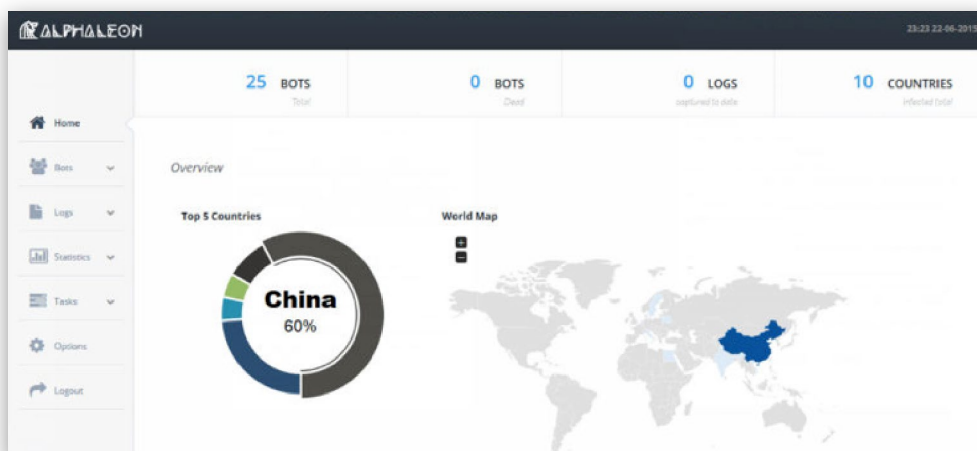
Most recently, Ganjaman advertised a new Android malware, "GM Loader," a tiny app which downloads additional malware on the phone. The software can be disguised as a legitimate app, such as an update from Adobe for example. These Android-based loaders have important implications, as botnets with loaders can be monetized by cybercriminals in malicious pay-per-install services.



GM Bot in Disguise

AlphaLeon

"AlphaLeon" is a prolific team of malware developers who are involved in the creation and sale of malware across several cybercrime forums. In 2015, the AlphaLeon team developed several different pieces of software. The most notable of these releases is the "AlphaLeon Bot Platform," announced in June.



AlphaLeon Control Panel

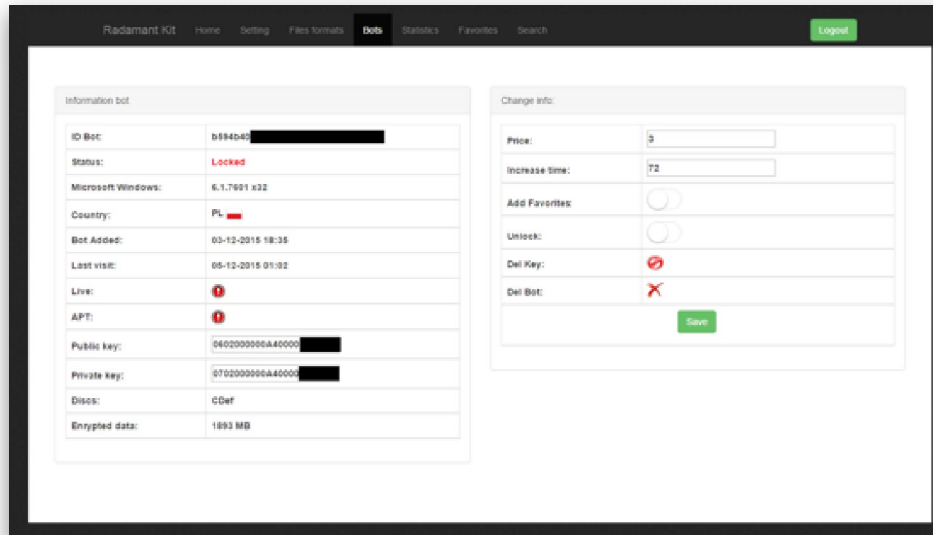
The platform includes the loader as the base product. Customizable plugins make the bot a versatile, multifunctional solution that offers criminals a range of options for converting their infections into income:

- Alpha-formgrab (IE, FF, Chrome, Opera, Safari)
- Alpha-softgrab (Email, FTP clients, Games, provided with login:pass)
- Alpha-vnc (Hidden VNC with back-connect functionality)
- Alpha-clicker (Ad-clicker, with embedded template customization)
- Alpha-spoof (DNS, Homepage, Browser web spoofer)
- Alpha-sock5 (Sock5 proxy tunneling with private port)
- Alpha-spread (Facebook, Myspace, Twitter, Reddit spreader)
- Alpha-rootkit (32bit, and 64bit rootkit for maximized bot security)
- Alpha-locker (ransomware, or scareware with customized settings)

Forum feedback indicates that the platform found a loyal following. Nevertheless, the team introduced a new product to the cybercriminal underground in October, this time a traditional banking trojan called "Anthrax." Purportedly developed from scratch rather than from leaked malware source code, the trojan supports web-injects, ring-3 rootkit, formgrabber, and encrypted communications.

Turnkey Ransomware

In December 2015, "Radamant" posted an advertisement for the "Radamant Ransomware Kit." On the client side, all storage devices are encrypted while hidden, and Windows restore files are deleted. The ransomware then deletes itself after



Radamant Control Panel

encryption is completed. The landing page for the client is available in 9 languages and includes a video showing the victim how to create a Bitcoin wallet and purchase Bitcoins. When the timer expires, the sum requested from the client doubles. On the server side, a unique bitcoin address is generated for each bot, with high levels of customization available for individual bots, including the ability to change the extension of encrypted files and encryption priorities. The entire software is only 70 kilobytes.

Conclusion

As Malware-as-a-service matures as an offering and authors continue to innovate with new malicious tools that are easily deployable by non-experts, the number of malware attacks will expand as non-technical actors take advantage of these packaged offerings.

Chinese Cybercrime – The Trend Towards Internationalization

Background

China has long been home to a relatively robust and large underground cybercrime community within the Deep & Dark Web. However, its structure and the behavior of its members have consistently differed significantly from those in other regions of the world. Throughout 2015, Flashpoint subject matter experts monitoring Chinese activity have observed increasing signs indicating the maturing and internationalization of the Chinese cybercrime underground.

Hacker forums have long been a staple of the Chinese Deep & Dark Web, but Chinese cybercriminals seemingly never adopted the forum model for other illicit activities, such as financially motivated cybercrime, in the same way as other underground communities. Instead, Chinese cybercrime has in large part relied upon the abuse of otherwise legitimate communications mediums and open boards such as Baidu Tieba and QQ messenger. In other cases, cybercriminals have been observed posting one-off advertisements for their services and wares on unrelated forums, such as those pertaining to discussions of real estate, education, video games and entertainment, and ethnic Chinese or Chinese nationals living abroad.

As a result of this model, illicit transactions within the Chinese underground have, up to this point, primarily taken place via a manual process – one-on-one engagements negotiated via private messages or instant messenger applications. This stands in stark contrast to the high level of professionalism and maturity that characterizes the Russian underground economy, where one-on-one transactions are primarily reserved for significant sales. The vast majority of mass retail business is conducted via automated shops and platforms designed to cater to a wide audience with little in the way of individual interaction between buyer and seller required.

Branching Out Internationally

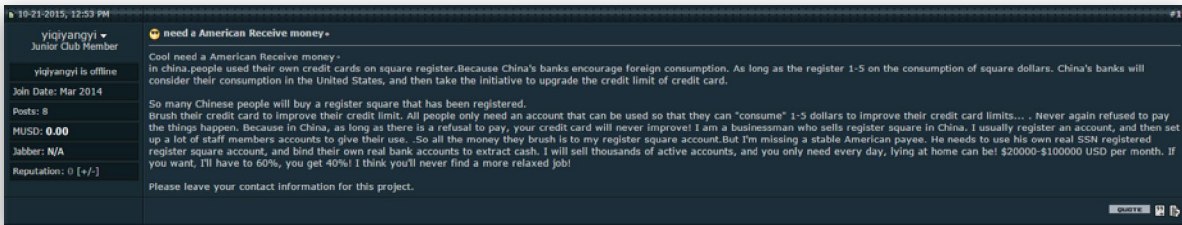
Throughout 2015, Flashpoint analysts monitoring disparate Chinese cybercriminal communities observed an increase in use of foreign-operated platforms, including forums and automated shops. Chinese cybercriminals appear increasingly drawn towards the use of prominent forums and shops within the Russian underground. One explanation for this phenomenon is likely found in the fact that many of these Russian-owned platforms may be described more accurately as “international” in

that they accept registration from non-Russians and have English-language sub-forums or shop interfaces, which reduces the barrier for entry for Chinese users, most of whom have a modicum of English proficiency due to the Chinese education system.



Posts on Baidu Tieba offering the sale of URLs on Russian payment card data shops, using Chinese transliterations of the original shop names

In tandem with the increase in use of foreign operated cybercrime shops, Flashpoint has noted an uptick in Chinese-speaking actors operating on international, yet Russian-run, cybercrime forums such as Lampeduza, Crdclub, and Infracard. On some occasions, such as in the screenshot below, the actors instead write in broken English in order to reach a wider audience, but maintain the use of Chinese cybercriminal slang, such as “to brush” (to swipe), in their posts.



“yiqiyangyi,” a Chinese-speaking member of Crdclub, soliciting for cybercrime partners in English

The Domestic Approach

Taking a page from the Russian model, some Chinese cybercriminals have established native Chinese communities or shops of their own. These platforms do not appear to have yet taken root in the broader international community. This low adoption is perhaps due to the ease of access to other already mature services, lack of effective marketing, and a fear of Chinese law enforcement. For example, in 2015, Flashpoint noted the launch



Chinese “Socks5 Http Proxy” shop interface

of the so-called Chinese “Socks5 Http Proxy” shop, the newly updated interface of which is depicted below, which serves as an automated marketplace for access to



Shuahuo173[.]com sub-forums

private Socks5 proxies, which are often used by cybercriminals for making illicit purchases with stolen payment card data.

Likewise, Flashpoint also observed the launch of Shuahuo173[.]com, a closed, pay-for-access Chinese-administered cybercrime forum dedicated to carding.

However, so-called “internet purification operations” (网络净化行动), conducted by the Chinese authorities to crack down on illicit behavior online within China’s borders will limit the growth of these native sites.

Conclusion

In 2016, Flashpoint subject matter experts expect to see a continuation of this trend toward automation within the Chinese community and the expanded use of foreign-operated cybercriminal platforms.

The French Underground – Managing Increased Media Visibility

Background

Throughout 2015, the handful of websites that make up the core of the French-language Deep & Dark Web grappled with the dilemma of how to remain true to their mission of creating an open and welcoming space despite increased media coverage that has attracted “undesirables” to the forums. These “undesirables” include law enforcement representatives, young kids attracted by the “cool factor” of being on the Deep & Dark Web, and users with little technical ability or understanding of how to maintain online anonymity. Flashpoint subject matter experts monitoring the underground French community’s activity have observed how this region of the Deep & Dark Web has developed measures to keep undesirables out while still remaining accessible as a community. These measures include the introduction of paywalls, required demonstration of technical competence, name changes, and a de facto tiered forum system.

The underground French community in the Deep & Dark Web, according to the community’s own historian (“hamster-guerrier”), began circa 2008 with an unmoderated forum called Noel Board.



French Deep Web Logo

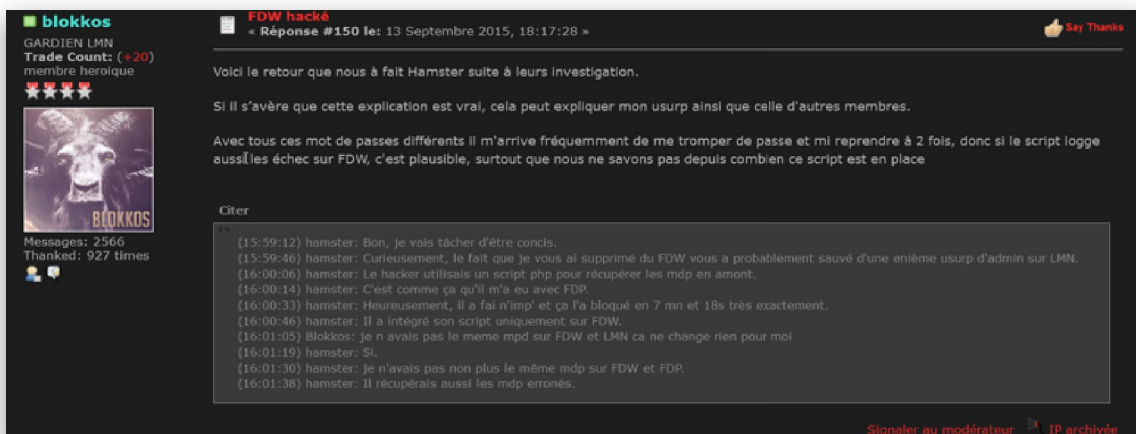
The chaos of this site eventually persuaded a user with the pseudonym “V1ct0r” to found the French Deep Web (FDW), a site dedicated to “providing a censorship-free forum for information exchange.” Following a law enforcement raid on the server hosting Noel Board, FDW has remained as the longest-standing and most stable presence in the French dark web.

Throughout its existence, FDW’s insistence on being a “safe space” for freedom of expression has played a central role in the forum’s development, with moderators policing only pedophilia and hate speech. And though cybercrime (primarily carding, scams, counterfeit currency, and falsified documents) has also become a mainstay of FDW and its derivative forums, they all serve primarily as outlets for information sharing, with market activities playing a secondary role.

Increased Media Coverage

The community's insistence on openness and free speech, however, has made it hard for the community's forums to deal with an influx of unwanted users who have been alerted to the forums' existence by French media outlets. According to hamster-guerrier, the first large wave of new members into the French Deep & Dark Web followed January 2014 reports in French newspapers Le Nouvel Observateur and Libération that were "linked to Edward Snowden's revelations." In hamster-guerrier's words, "this brought in a large quantity of amateurs and tourists," though it also had the positive benefit of causing "an explosion in the number of Tor connections dramatically increasing the speed of the network."

The media coverage continued in 2015, the most notable example of which was the hacking of FDW and attacks against other underground French forums, which led to coverage in the prestigious French daily, Le Monde, and the French-language security publication, ZATAZ. During this period, Flashpoint subject matter experts observed that members of the forums debated measures to keep themselves safe and anonymous.



"hamster-guerrier" describes the investigation of the hack that occurred against FDW

Measures to Deter Undesirables

- **Restricting Access**

FDP severely restricted membership and even deleted the profiles of non-active members going from approximately 950 members to 220 members.

- **Paywalls**

When Black Hand opened in February 2015, it became the only forum of the French underground to require paid membership. The amount is not high (about 20 euros), but it accomplishes a few goals. First, it discourages registration by visitors who are

only curious and are less likely to pay just to browse the forum. Second, it discourages users from making multiple accounts, a common complaint in online communities. And third, it ensures that potential members at least have the technical competence to conduct transactions using bitcoin, slightly raising the selectivity of the forum.

- **Technical Competence**

Beyond the competence required to transact in Bitcoin, Black Hand, FDP, and IBM now require registrants to submit a profile detailing other Deep & Dark Web forums they are members of, the length of their membership on those forums, an explanation of the measures the registrant uses to maintain anonymity (which operating systems, what kind of VPN, presence or not of a virtual machine, etc.), and PGP key (to demonstrate that the registrant can send and receive encrypted messages). These newly introduced requirements help moderators set a higher barrier for entry to registrants uninitiated in the basic tools of the forum.

- **Name Changes**

Following the ZATAZ and Le Monde reports in October 2015, administrators of La Main Noire decided to change the name of the forum to its English translation, Black Hand, as well as forum logo. This was intended to frustrate attempts by curious visitors who likely would not realize that Black Hand and La Main Noire were one in the same. Administrators also introduced two-factor authentication for member logins.

- **De Facto Tiered System**

Given the introduction of new security measures across the French Deep & Dark Web underground and the closeness of the community, a tiered forum system has evolved whereby certain forums (e.g. FDW) are easy to find and join, and provide information to new users on how to survive and thrive in the Deep & Dark Web. Other forums (FDP, IBM) require registrants to demonstrate their activity in other underground French forums, allowing administrators to check on registrants to determine their overall participation in the forum, as well as the type and tenor of their activities.

Conclusion

The cumulative effect of these measures, more by accident than by design, has been to create a pipeline for any underground French users to enter, learn, and gain access to higher value Deep & Dark Web forums. This has made it easier for moderators to direct the flow of visitors while avoiding being inundated with undesirable members who would likely dilute the quality of the forums. In this way, the French Deep & Dark Web community is inclusive to all, while still able to remain selective. Of course, the community itself has been anything but stable, so it remains to be seen how long this system holds, and how the community will continue to respond to the external pressures of media coverage.

Hactivists & Chaotic Actors

Background

2015 has been an active year for hactivists using techniques such as Doxing, Swatting and DDoS attacks. Flashpoint subject matter experts monitoring the Deep & Dark Web believe a second category should be included in this assessment: The apolitical chaotic actor – an attacker who is not motivated by politics or money but is instead motivated by fame, ego, or attention. Flashpoint subject matter experts have noticed that a number of attacks did not fit the purely political motivations normally ascribed to hactivism. The “chaotic actor” is not a new concept and has been used before to describe hactivists, but for the purposes of this report, they are considered to be apolitical.

Doxing Is Becoming Popular

Doxing, the publishing of personal or identifying information, is rising in popularity. Unlike most forms of cyberattack, doxing has potentially dangerous physical consequences. These attacks often cannot be prevented because there are usually no processes in place for removing oneself from public records. Doxing is closely associated with swatting and account hijacking, and published dox are often used to incite harassment or physical attacks. The motivations for doxing are varied and often political.

Flashpoint has observed a number of significant doxing related events in 2015. Their victims include:

- A large number of police officers for various reasons by activists
- An American dentist for a legal lion hunt
- Members of the Ashley Madison cheating site after their database was dumped
- Members of the KKK, an organization with a traditionally secret membership
- Members of the US military by ISIS supporters
- Adults and underage children to extort graphic pictures or money

Some doxes are more complete than others. Some dox contain social security numbers and all the information needed to take over the victim's identity. Sometimes a victim has to deal with multiple cases of identity theft all stemming from a single doxing event.

Doxbin, a Dark Web repository of doxes, was taken down in an FBI operation. Doxbin was infamous for several years for enabling harassment of the people named on the site.

Awareness of Swatting Is Increasing

Swatting, the dispatching of police to a victim's address under false pretenses, originated in the phreaking community as a prank. With the spreading knowledge of the attack and how to do it, swatting has become more popular in recent years. Nowadays, the technique is widely known in the hacking community, and is a preferred harassment technique of some individuals. The typical person arrested for swatting is a male under 25. Mental illness or a history of abuse is a common factor. Those arrested for swatting are often serial swatters who have performed dozens of calls. Swatting has received recognition in the media, and this attention provides a significant motivation for some serial swatters.

A number of legal issues are at play that make it more difficult for law enforcement to address swatting. Swatting is often committed by juveniles across international boundaries. Even if the perpetrator's identity is discovered, many countries will not extradite minors. Some countries do not yet recognize swatting as a serious crime. Some swatters understand this and act with impunity. Awareness of swatting is increasing and legislation is being proposed, such as the "Interstate Swatting Hoax Act of 2015".

DDOS Is Getting Worse

DDOS or Distributed Denial of Service attacks require a significant number of exploitable machines. The proliferation of "Internet of Things" devices with default administration passwords has created a surplus of exploitable machines that are difficult if not impossible to patch. A glut of "booters" (cheap DDOS-for-hire web applications) over the past several years has made DDOS attacks accessible even to people without technical skills or connections to the underground. Not only has DDOS gotten cheaper, but the high water mark for large attacks has gotten higher. Until "Internet of Things" devices are designed without default remote administration passwords, DDOS attacks will continue to get worse.

Chaotic Attacks Continue to be Fueled by the Media

Chaotic attacks are characterized as attention seeking behavior with no more than a veneer of political speech. It is sometimes mistaken for political hacktivism. Significant chaotic attacks in 2015 included:

- The hack of TalkTalk by juveniles and young adults living in the UK.

- The hack of the Director of the CIA John Brennan's personal email and FBI Deputy Director Mark Giuliano's personal email, and the unauthorized log in to FBI's Joint automated Booking System by the hacktivist group CWA.
- Lenovo, Google.com.vn, Malaysia Airlines, Tesla were hacked and defaced by Lizard Squad.
- A teenager from Coquitlam, Canada, was arrested on numerous charges of swatting and bomb threats. One of his bomb threats shut down Disneyland.
- Matthew Tollis of Connecticut was sentenced to a year in prison for multiple swatting attacks, including a bomb threat to the University of Connecticut.
- A New Jersey lawmaker attempting to stiffen penalties for swatting was swatted.
- The closure of 1,087 schools in Los Angeles over a single e-mail threat.

Chaotic hackers often aim for the "low hanging fruit" of easy hacks against the most impactful victims. As long as there are companies with poor security practices, there will be chaotic hackers taking advantage of the opportunity. Chaotic actors are often motivated by the excitement and adrenaline rush. The media coverage and attention play heavily into the motivation to continue their behavior as well as inspiring copycats to imitate effective attacks. Awareness of this fact is important in the process of de-escalating a situation. With the rise of ISIS and fears of terrorism, chaotic actors may find that they can easily provoke a media reaction by pretending to be ISIS or by making fake terrorist threats. It will be important to differentiate between jihadists and people who simply invoke terrorism for attention.

Conclusion

Both politically motivated hackers and chaotic actors continue to be a concern in the upcoming year. Unlike jihadists or financially motivated attackers, these types of attackers have a great diversity of motives and are therefore more difficult to predict. Many of the attackers in this group are underage, with low impulse control and a proclivity for risk-seeking that make them dangerous and unstable adversaries. It is important to be aware that these types of actors are driven by the news, and the news is driven by them – creating a vicious cycle. Any strategy in dealing with these actors must take this cycle into account.

Jihadi Underground Forums – Shifting Alliances

Background

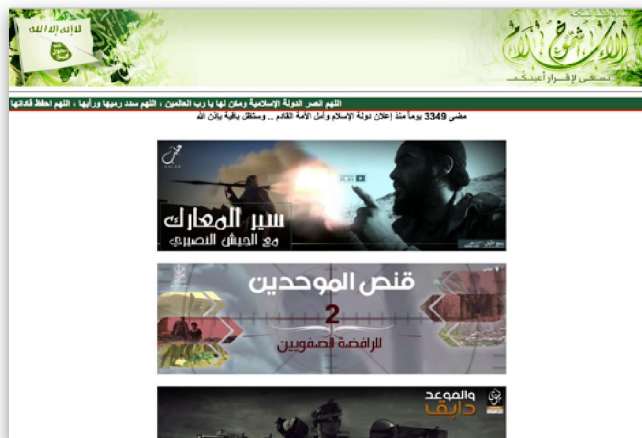
Flashpoint subject matter experts monitoring illicit jihadist and terrorist activities in the Deep & Dark Web have observed a number of trends in these shadowy areas of the Internet, particularly in relation to The Islamic State (ISIS) and its online presence, as well as the activities of its online supporters.

As events transpire on the ground, whether in Syria, Iraq, Libya, or other areas plagued by ISIS's rise, chatter on the Deep & Dark Web echoes these developments, including ISIS's territorial advancement, its battles with other fighting factions, and the growth of its media units and online platforms.

Shifting Towards ISIS

Shifting allegiances on the battlefield have overwhelmingly unfolded in ISIS's favor as the group has attracted foreign fighters from more than 80 countries and received pledges of allegiance from other terrorist groups, jihadist cells, and radical individuals. A number of groups that were either officially allegiant to, or were presumed to be allegiant to Al-Qaida have pledged their allegiance to ISIS leader Abu Bakr Al-Baghdadi. Many did so publicly, swearing an oath of allegiance in audio, video, or written statements.

These shifting allegiances in the physical realm have also materialized online, culminating in a relatively consistent trend observed over the course of the last year and a half. The most prolific and prominent Deep Web jihadi forums, which had supported Al-Qaida's online activities for years,



Official ISIS Forum "Shumukh Al Islam Network"

including the dissemination of propaganda, have shifted their loyalties and publicly pledged allegiance to ISIS leader Al-Baghdadi. These web forums include Shumukh Al-Islam Network, the longest standing jihadi web forum. This platform has been the top jihadi networking site in the Deep Web since 2009, and its administrators have persistently supported Al-Qaida. Late last year however, they pledged allegiance to ISIS, subsequently becoming the group's official web forum where its propaganda is first posted and then propagated.

Even previously defunct jihadi web forums that have been absent for at least two years recently resurfaced, returning with hardline support for ISIS. For instance, Atahadi Islamic Network and Leyoth Islamic Network - two web forums that supported Al-Qaida's propaganda dissemination for years - returned online as ISIS supportive web forums and media units, removing previously distributed Al-Qaida propaganda and making space for official ISIS videos and documents, articles, and other material that supports ISIS ideology.

Adding to the growing ISIS cyber landscape, new web forums in support of the group began surfacing earlier this year. The emergence of these new forums, such as Islamic-DW and IslamicState.pro, further exemplifies the shifting winds of allegiance within the jihadi community.

Technically Savvy Jihadists

The ISIS supportive community is also responsible for another significant trend in the jihadi underground: the growth of increasingly technically savvy jihadists. This has been demonstrated by the uptick of pro-ISIS hackers who have amplified their attacks on Western government, military, and financial targets. Although this has been carried out with negligible success and minimal sophistication thus far, this tactical evolution presents a growing threat in the future as jihadists continue to foster these skills.

In addition to the aforementioned hacking efforts, self-proclaimed technologists supportive of ISIS have established safe havens in the Deep Web. For instance, one of these actors, who focuses on cyber security and supports ISIS, established his own



Pro ISIS User Issues Manual on Encrypted Communication Tool

Deep Web forum, where he posts manuals and guidelines on various tech and cyber issues, tools, and software.

Conclusion

The growing strength of ISIS within the jihadist community in 2015 has been echoed in growth of their online presence. The growth of their online presence is also resulting in a growing community of tech-savvy jihadists. As these tech-savvy jihadists gain expertise, they represent a greater threat to Western government, military, and financial targets.

The “Crypto-Wars” and Tor Hidden Services

Background

The 2016 U.S. Presidential primary debates, along with recent terrorist attacks, have drawn a large amount of attention and interest to the issue of encryption and secure communications tools. As a result, the “crypto-wars” have reignited. However, since it is not possible for the U.S. government to remove encryption technology from the public domain, this attention will likely only result in free advertising for encryption apps and an increase in operations security (OPSEC) awareness amongst most users, including those who use encryption for malicious purposes. At the same time, there has been a growth in the use of privacy protocols such as Tor and I2P in the Deep & Dark Web. Flashpoint subject matter experts have been tracking usage of these hidden services and have observed significant growth in 2015.

The Encryption and Backdoor Debate

In what may be the Golden Age of Intelligence, with more information available than ever before, government and law enforcement officials continue to express dissatisfaction with the limitations on the available data. Part of the debate centers around privacy protocols, such as Tor and I2P, which offer their users enhanced anonymity online, but also frustrate law enforcement efforts aimed at tracking and cracking down on illicit activities. These tools are not new—having been in existence for over a decade—but the debate on their legitimacy is once again coming into the fore, against a backdrop of transnational terrorism, the expansion and industrialization of the illicit drug trade, and the battle against cyber espionage.

As a result of the increasing attention paid by politicians to the encryption debate and online communities, the issue is very much becoming more widely understood amongst the populace and is thus increasingly likely to serve as a hot-button point of contention between the opposing sides of the security-versus-privacy debate.

Dark Web Density

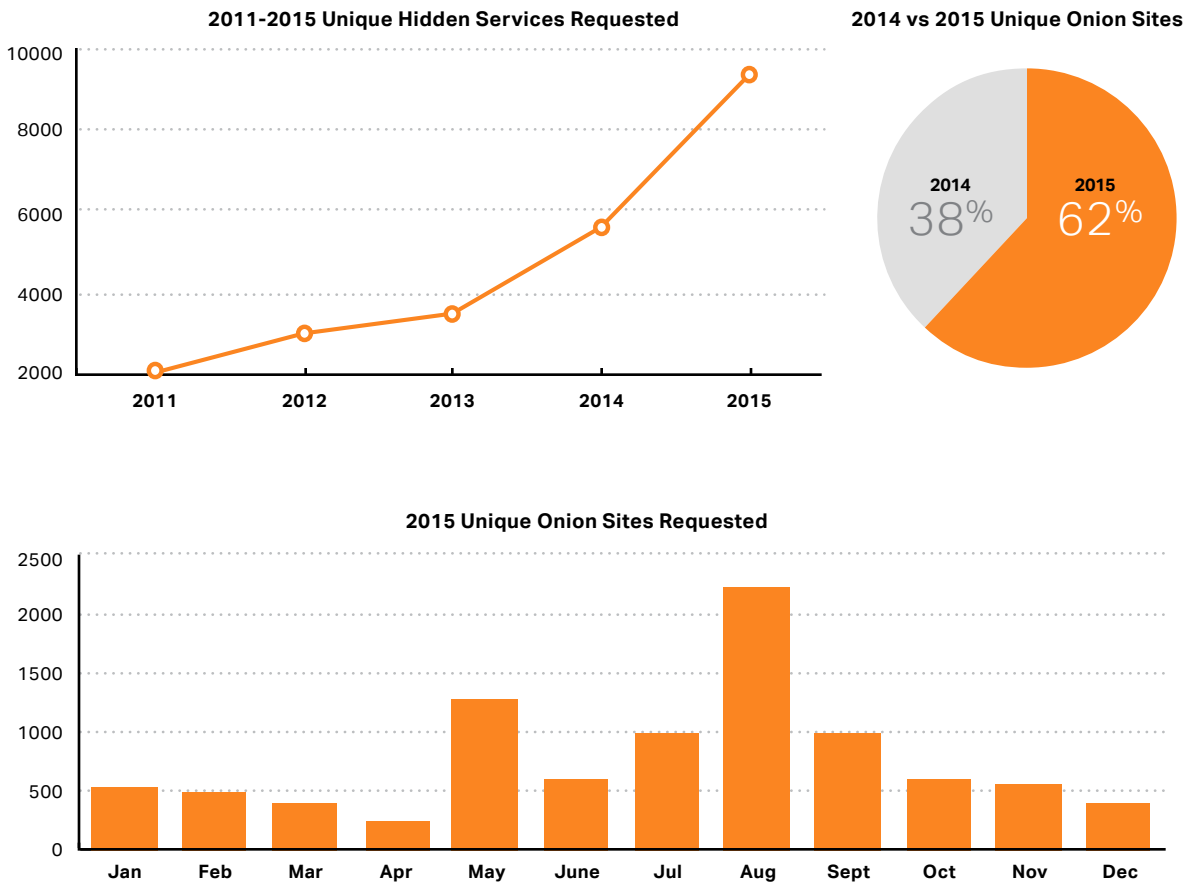
Despite a myriad of arguments that have been advanced detailing how encryption is causing a loss of visibility into online activities, Flashpoint has been compiling vast amounts of information from a large number of criminal and jihadist forums, many of which are only available via encrypted Tor hidden services. This number is increasing as new hidden communities are discovered and collected for analysis.

.onion Survey

Flashpoint conducted a survey across all detectable Tor hidden services over a specified time range. The research was based on passive DNS data sets¹ showing requests by Internet users to multiple publicly available web-based tor2web proxies to gain an understanding of the estimated growth of Tor hidden service usage over the past 5 years. We sampled the data across the proxies and found that the general numbers remained consistent, so we normalized the data sets with certain caveats:

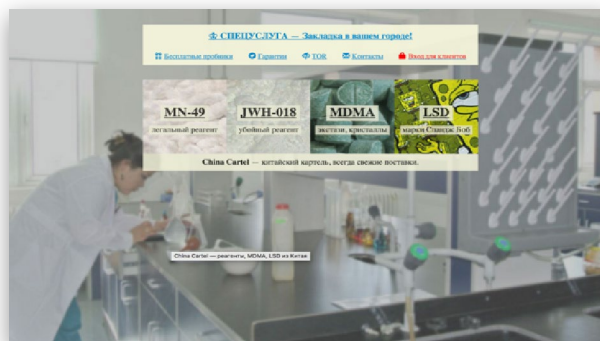
1. The requests and their numbers may be affected by outages from time to time
2. This is only based on users who make requests through these open web services and does not reflect all hidden service traffic
3. This is a sample set and is designed to give a general estimate based on observations
4. The data reflects the time period between January 1, 2011 and December 31, 2015

Based on the data set it appears that unique Tor hidden service first-sightings increased at a steady rate in the past 4 years.



¹ Based on Farsight Security-provided pDNS data.

In the past year there was a 24% increase in unique hidden services that went online. An interesting burst of activity that was observed in 2015 was a dramatic increase in unique Tor services after July 2015. While investigating news regarding underground activity between June and August 2015, we noted that the Darkode takedown was announced in July 2015, and may thus be one factor explaining the increase of Tor hidden services during that time.



The homepage of "China Cartel," an underground illicit drugs market

Although privacy is the primary argument for the use of tools such as Tor, the most popular traffic requests on the Tor network appear to be malicious or illicit in nature, such as drug distribution or child pornography sites, and CryptoWall ransomware payment servers.

Conclusion

Given the public discussion on the topic, use of privacy protocols such as Tor and I2P will continue to increase. Governments will find it difficult to legislate and exert control over encryption and privacy protocols available in the public domain.

Final Conclusion

While the Deep & Dark Web only represents a portion of the entire web, the activity that is conducted in this largely unmonitored and inaccessible space may just be the most important activity for you to be concerned with, posing the greatest risk to your organization and critical assets.

With our direct portal to this world, Flashpoint Subject Matter Experts are in a unique position to detect increasing threat levels, as well as identify never before seen schemes and plots. To recap, here are the most prolific trends of 2015 that we identified across various recurring forums, communities, and themes:

- 1. Anyone Can Be a Cybercriminal.** With lower barriers to entry and less technological savvy required, the profile of a fraudster has expanded, as well as the tool set—such as the variety of malware-as-a-service offerings—available to empower them.
- 2. Just Say No.** Drugs are still bad, and more desirable and accessible through dark net markets than ever before, resulting in 50% of all Tor markets offering narcotics. The growth in online drug markets will cause increased interest in dark net markets.
- 3. The Public Domain Is the Wild West.** With conversations on encryption and privacy entering the political realm, and with no legislature or governance in place addressing the usage of hidden services, the uptick in Tor and I2P services will continue, and so will the exploitation of these services to conduct illicit and malicious activity.
- 4. Not the Fortune, but the Fame.** The politically and financially motivated actors are still a threat to all governments, organizations, and individuals that don't line up with their agenda. But another dangerous actor group has emerged in 2015, those motivated by chaos and fame. Their actions and goals are much more challenging to predict.
- 5. Cybercrime and Terrorism without Borders.** The internationalization and globalization of cybercrime is inevitable. In 2015, we saw Chinese communities automating with real force for the first time—and—expanding internationally, taking their business to Russian forums. 2015 also saw the rise of Jihadist communities continuing to leverage Deep & Dark Web forums. These communities have been invigorated with younger, more tech-savvy talent with a strong support for ISIS, creating an increased risk to the West, and farther reach for ISIS.

By distilling our observations from within the Deep and Dark Web, this report highlights the growing complexity of illicit communities and the industrialization of cybercrime in 2015. This threat intelligence, we hope, will aid decision makers and analysts alike in better understanding and anticipating the dangers posed by illicit actors to their organization.

Learn More

Interested in learning more about the types of threat intelligence Flashpoint collects and how it can be applicable to your business? We encourage you to contact us directly at intel@flashpoint-intel.com. Our team can address those risks that are of immediate concern to your industry, including but not limited to: Finance, Retail, Technology, Pharma, Government, Energy, and more.

To learn more about how Deep & Dark Web data can help shed light on threats that could severely impact your organization, we invite you to explore our paper, ["Illuminating the Deep & Dark Web"](#).

About Flashpoint:

Flashpoint provides the reports, tools, data, and access to experts necessary to obtain tactical, operational, and strategic intelligence from the Deep & Dark Web. The company offers a state-of-the-art platform with data curated by world-class subject matter experts. Flashpoint's products illuminate threatening actors, relationships, behaviors, and networks concealed within these hidden areas of the Internet. Security and intelligence teams across the Fortune 500 and government use the company's data, tools, and expertise to reduce the costs of fraud, data loss, reputational damage, or other attacks. Flashpoint is backed by TechOperators, Greycroft Partners, K2 Intelligence, Bloomberg Beta, and Cisco Investments.

Visit us at www.flashpoint-intel.com to learn more.