THE LIFE STORY OF AN IPT – INEPT PERSISTENT THREAT ACTOR

Adam Haertlé
BadCyber.com, Poland

Email adam@badcyber.com

ABSTRACT

This paper describes the ability of an amateur attacker with no technical skills to achieve success in his criminal enterprise. We will follow a Polish threat actor, known as 'Thomas', in his career as a wannabe cybercriminal from late 2011 until today. We will watch his first steps on HackForums (HF), where friendly vendors and free tools help him to build his first botnet. We will follow his phishing and spam campaigns visible in the media and correlate them with tool purchases on HF. We will see how his tools evolve and his botnets grow despite his total lack of technical and language skills. We will celebrate with him as he brags about his successes and commiserate with him over his failures, as he attempts to pivot into banking fraud and gets scammed by others on multiple occasions. We will look at his business strategies and monetization vectors, including a botnet-as-a-service offering, while contemplating pricing strategies and ad design skills. We will discover his identity though multiple uncensored screenshots and end by trying to explain the legal hurdles which mean that, despite being well known to the law enforcement community, he remains at large.

INTRODUCTION

The prevalence and ease of availability of multiple tools used to commit cybercrimes creates a friendly environment even for the beginner criminal. One of the most popular places to obtain hacking tools and help from the hacker community dominated by criminal intent is HackForums [1]. This also happens to be where the subject of our paper created his account, on 1 August 2012 [2]. Initially, he used the pseudonym 'Armaged0n', which later changed to 'the.xAx'. While Internet search results reveal that his first documented attempt at Internet crime might have involved setting up a fake online shop offering mobile phones at discounted prices in October 2011 [3], it looks like it was his participation in the HackForums community that really kick-started his criminal career.

FIRST BOTNET

The first posts authored by Armaged0n on HackForums show a clear direction in his actions, which are aimed at building and deploying his first botnet. In September 2012 he is looking for free services, including botnet set-up, crypter, VPS, VPN and binder [4]. While he manages to obtain some of the requested tools and services for free, a few days later he decides to purchase the botnet set-up – while at the same time revealing his *Skype* username, including his real surname. His product of choice is the Athena IRC botnet [5]. After some trouble with the set-up he obtains professional help from the vendor and the botnet C&C goes live. Two days later, Armaged0n runs two spam campaigns to spread the botnet client, the messages impersonating both *Kaspersky Lab* [6] and a popular Polish Internet auction brand, *Allegro* [7].

The next day, Armaged0n publishes a comment on a blog site describing his spam campaign. In it, he admits to having been the author of both *Kaspersky Lab* and *Allegro* messages and posts screenshots with statistics detailing both landing page visits and botnet C&C traffic, together with his *Skype* username.

He also claims to have infected 900 victims, while the screenshots show fewer than 100 active bots. He mentions that he is planning to use his botnet for DDoS attacks and Bitcoin mining, and a few days later he posts on HackForums, looking for a Bitcoin miner client to run on his botnet victims' computers [8].

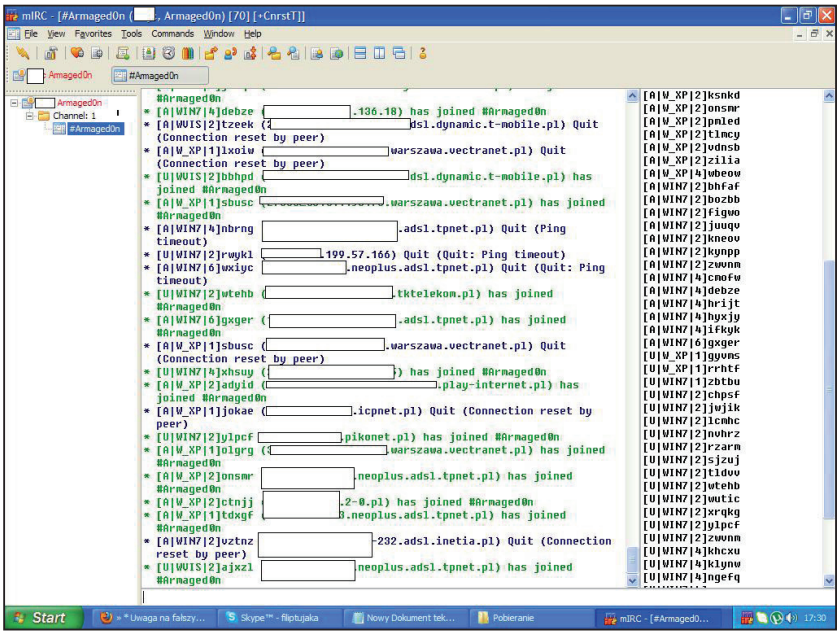

Figure 1: Botnet C&C traffic.

GROWING FRUSTRATION

His subsequent posts on HackForums show a growing level of frustration. He runs into technical issues with remote access trojan (RAT) connectivity [9] and with a crypter for his botnet [10]. The most painful mistake comes to light on 20 October, when Armaged0n loses control over his botnet. His VPS provider changes hosting location, which causes a change in the IP address of the C&C server and subsequent loss of connectivity with infected victims. This is the day on which Armaged0n learns about dynamic DNS services and starts using them for future botnet C&C servers [11].

To rebuild his botnet he runs new spam campaigns, impersonating *Allegro*, *PayPal* and *Facebook* [12–14]. All of the messages try to persuade the end-user to download and run the botnet client. While the *Allegro* and *PayPal* spam messages end with the usual phrase used in Armaged0n's spam runs ('Best regards [brand name]'), the *Facebook* one ends with 'Andrew Jones, Stewardship Monitoring Section, Security and Server Administration Department Facebook.pl'. This significant change in style can be attributed to one of the blog comments beneath the description of the *PayPal* attack, saying:

> 'Why can't the scammers do their job properly? "Best Regards PayPal Group" – why not rather use something like "Andrew Smith, Stewardship Monitoring Section, Security and Server Administration Department"?'

It can be concluded that Armaged0n takes the commenter's advice on board and implements it in most of his future spam runs over the next two years.

FIRST MONETIZATION VECTORS

At the beginning of 2013, Armaged0n's first attempts at monetization of criminal activity can be observed. In January 2013, he tries to phish for banking credentials, impersonating the largest Polish bank, *PKO BP*, (see Figure 2) while also trying to steal one-time codes [15].

In February 2013, he puts up an offer of stolen *Steam* accounts on HackForums [16]. In May 2013, he tries to mine Bitcoins with around 120 infected machines [17]. In July 2013, he starts offering the 'Armaged0n Spam Service', pricing it at US$4 per 10,000 messages [18].

ANDROMEDA BOTNET

Also in July 2013, he decides to run an Andromeda botnet. He purchases the botnet set-up service from a vendor for US$6 [19]. We have not identified his bot-spreading method on this occasion, but it must have been very effective. By 15 August he has successfully infected 2,850 victims. Two days later, the number has grown to 3,205 infections (Figure 3), and by 19 August the botnet has reached 3,500 clients. Armeged0n puts the botnet up for sale for US$100 [20].

On 23 August, a small Polish ISP announces that it is the victim of a DDoS attack [21]. Although the attackers act under the pseudonym of '2Pac Team', we are confident that this is another of Armaged0n's identities. At the same time, he runs several DDoS attacks against multiple Polish companies, including a hosting provider, where he hosts the C&C of his botnet. The hosting provider takes immediate action and Armeged0n loses his botnet for the second time.

SCAM VICTIM

While working with scammers on HackForums, Armaged0n becomes a scam victim himself. On 20 August he offers for sale a GB£72 *Ukash* voucher, but another HackForums user takes the voucher and disappears without making the payment. Argmend0n files an official complaint, but never receives his money back [22]. A few weeks later, he is looking for the services of a programmer – he wants someone to help him create a simple tool to swap bank account numbers in the operating system's clipboard. The tool is modelled after other similar malware samples discovered in Poland a few months earlier. The vendor of the services turns

Figure 2: Bank phishing.

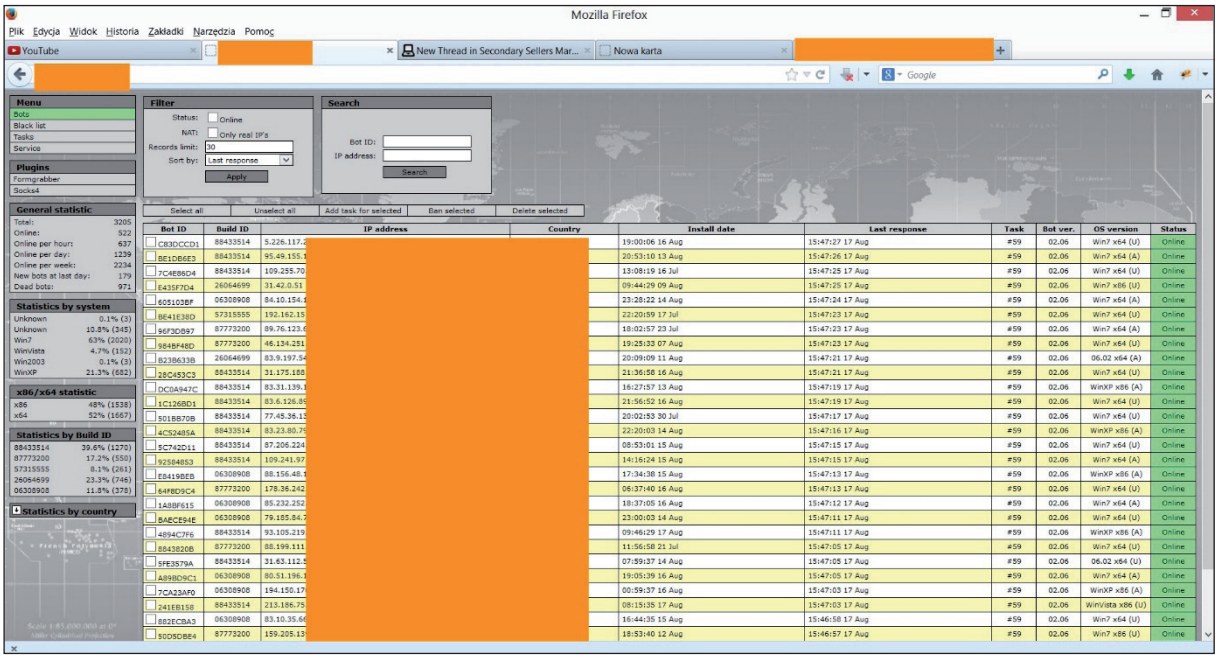

Figure 3: Andromeda panel.

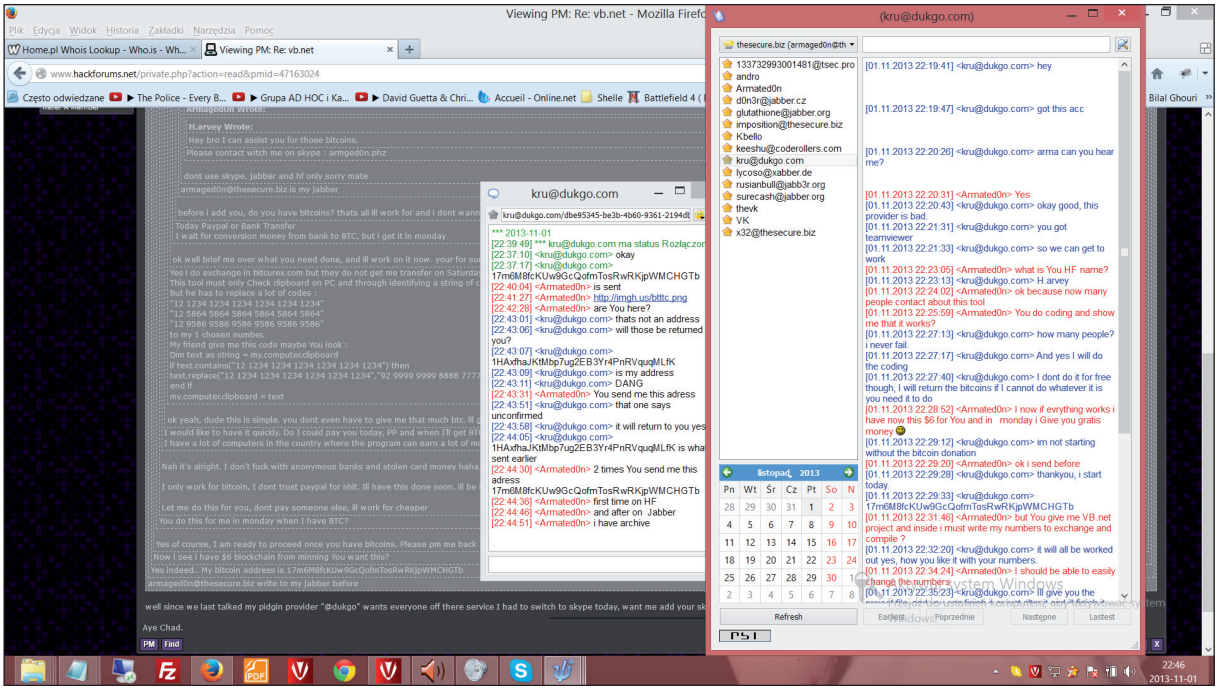

Figure 4: Original screenshot.

out to be another scammer, taking US$6 and never delivering on his promises [23]. While providing screenshots from the conversation with the scammer, Armeged0n obfuscates critical parts of the screen, however the screenshot is hosted on an external website, and if one changes the filename from 'arch_19.png' to 'arch_18.png', an original screenshot without any obfuscation can easily be obtained (see Figure 4).

Armaged0n does not give up on the idea of using malware to change bank account numbers in the clipboard, and in March 2014 makes a second attempt at purchasing relevant code [24]. That attempt must have been successful because in May 2014, CERT Polska describes a simple 'VBKlip' tool, very similar to the one ordered by Amaged0n, distributed by the Andromeda botnet [25].

MACRO ATTACK

In May 2014, Armaged0n starts using *Microsoft Office* documents with malicious macros to attacks users. The first documented attempt takes place on 4 May and is directed at readers of a Polish security blog. The malicious *Word* file linked from a *Facebook* post pretends to contain information about an alleged hack of a Polish Bitcoin exchange, and downloads and runs malicious files from an external server.

Multiple examples of similar attacks are launched over the next few weeks, including debt collection templates, alleged data leaks from a popular Polish website, and another spam campaign targeting *Allegro* users. This time the message content is largely improved through personalization, and it targets selected *Allegro* vendors.

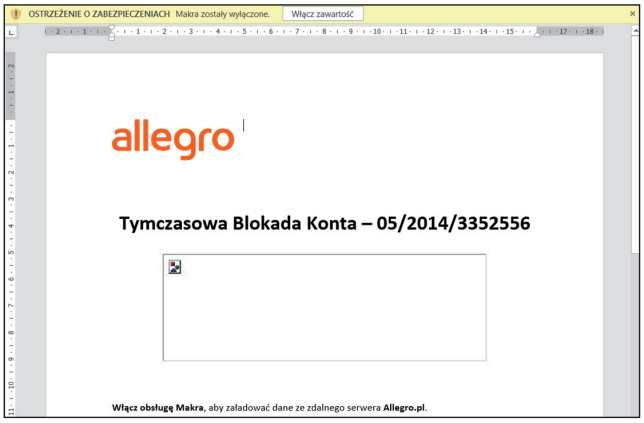

Figure 5: Allegro malware campaign.

It is worth noting that the *Office* document properties include the username 'Thomas', which is the English form of the original Polish name Tomasz, which is the real first name of Armaged0n.

MORE BUSINESS OFFERS

In July 2014, Armaged0n becomes so proficient at configuring new botnet instances that he starts offering botnet set-up services himself. His offer looks attractive – Andromeda set-up with EU domain for 12 months, including hosting in 'East EU', 99.99% uptime, 24/7 support and DDoS protection – all for only US$10 [26].

Also among his commercial offerings are *Microsoft Word* attacks, where the customer can easily 'convert' EXE and JAR files to *MS Office* DOC files. In December 2015, he offers two types of attacks – 'Macro' (US$39) and 'Silent' (US$399) [27]. Both include a bulk mailer, free crypting, full malware compatibility, x32 and x64 compatibility, and *TeamViewer* support. However, the movie demonstrating the 'Silent' exploit reveals that in order for the exploit to succeed, the user needs to click and approve the macro to run. Just before the movie ends, the viewer can get a glimpse of Armaged0n's desktop, including icons for many of the tools, malware samples and address lists he keeps using (see Figure 6).

EPILOGUE

While Armaged0n's actions are well documented and his identity is known to Polish law enforcement agents, he resides in another EU country and, despite several attempts to address this issue, he remains at large. There seem to be a lot of legal and operational hurdles to overcome to bring him to justice in Poland, where most of his victims are located.

Unfortunately, in April 2016, Armeged0n's account on HackForums was banned, probably for trading in stolen credit card data. While we can still observe active, ongoing malware campaigns that can be attributed to him, we have not identified his new account name and can no longer correlate these campaigns with HackForums purchases.

REFERENCES

[1] http://hackforums.net/.

[2] https://hackforums.net/member.php?action=profile&uid=1407151.

[3] http://katalogi.pl/106443-oszukani-przez-sklep-wwwnotoverpaypl.html.

[4] https://hackforums.net/search.php?action=results&sid=e3961281088e72443b1848044af05ae6.

[5] https://hackforums.net/showthread.php?tid=2753857&pid=26607049#pid26607049.

[6] https://www.kaspersky.pl/o-nas/informacje-prasowe/1797/spamerzy-podszywaja-sie-w-polsce-pod-kaspersky-lab.

[7] https://niebezpiecznik.pl/post/uwaga-na-falszywe-maile-od-allegro/.

Figure 6: Armaged0n's desktop.

[8] https://hackforums.net/showthread.php?tid=2677567&pid=26714719#pid26714719.

[9] https://hackforums.net/showthread.php?tid=2947810.

[10] https://hackforums.net/showthread.php?tid=2772969&pid=27331378#pid27331378.

[11] https://hackforums.net/showthread.php?tid=2884400&pid=27425019#pid27425019.

[12] https://niebezpiecznik.pl/post/twoje-konto-w-allegro-pl-zostalo-zablokowane/.

[13] https://niebezpiecznik.pl/post/uwaga-na-falszywe-e-maile-od-paypala/.

[14] https://niebezpiecznik.pl/post/wlamanie-na-twoje-konto-facebook-www-odzyskajfacebook-tk/.

[15] https://zaufanatrzeciastrona.pl/post/wykrylismy-probe-wlamania-na-twoje-konto-bankowe-ipko/.

[16] https://hackforums.net/showthread.php?tid=3267934.

[17] https://hackforums.net/showthread.php?tid=3199046&pid=32384643#pid32384643.

[18] https://hackforums.net/showthread.php?tid=3566869.

[19] https://hackforums.net/showthread.php?tid=3599327&pid=33818742#pid33818742.

[20] https://hackforums.net/showthread.php?tid=3697521&pid=34705612#pid34705612.

[21] https://plus.google.com/101407041154547721013/posts/3Umqs4XrYoM.

[22] https://hackforums.net/showthread.php?tid=3705186.

[23] https://hackforums.net/showthread.php?tid=3813506.

[24] https://hackforums.net/showthread.php?tid=4142088.

[25] https://www.cert.pl/news/single/podsumowanie-zagrozenia-vbklip/.

[26] https://hackforums.net/showthread.php?tid=4353434.

[27] https://hackforums.net/showthread.php?tid=5098527.