Growth and Commoditization of Remote Access Trojans

Veronica Valeros
Department of Computer Science
Czech Technical University
Prague, Czech Republic
valerver@fel.cvut.cz

Sebastian Garcia
Department of Computer Science
Czech Technical University
Prague, Czech Republic
sebastian.garcia@agents.fel.cvut.cz

***Abstract*—In the last three decades there have been significant changes in the cybercrime world in terms of organization, type of attacks, and tools. Remote Access Trojans (RAT) are an intrinsic part of traditional cybercriminal activities but they have become a standard tool in advanced espionage and scams attacks. The overly specialized research in our community on Remote Access Trojans has resulted in a seemingly lack of general perspective and understanding on how RATs have evolved as a phenomenon. This work presents a new generalist perspective on Remote Access Trojans, an analysis of their growth in the last 30 years, and a discussion on how they have become a commodity in the last decade. We found that the amount of RATs increased drastically in the last ten years and that nowadays they have become standardized commodity products that are no very different from each other.**

***Index Terms*—remote access trojans, underground economy, cybercrime, marketplaces, malware, commoditization**

1. Introduction

Remote access software is a type of computer program that allows an individual to have full remote control of the device where the software is installed. *Remote Access Tool* refers to a type of remote access software used for benign purposes, such as TeamViewer [1] or Ammyy Admin [2], which are common tools used by billions of users worldwide. *Remote Access Trojans* (RAT) are a special type of remote access software commonly used for malicious purposes, where (i) the installation is done without user consent, (ii) the remote control is done secretly, and (iii) the program hides itself in the system to avoid detection. The distinction between tools and trojans was created by the information security industry to distinguish benign from malicious RATs, however in the underground, attackers claim all RATs are *Remote Access Tools*.

Early Remote Access Trojans were used for pranks and for fun, to showcase skills, and to brag in hacking forums. Developing your own RAT was an entry level skill that inexperienced users were somehow expected to rapidly acquire. Websites like megasecurity.org were used to list and publish new RATs, many of which were never developed further. While the challenge of building highly functional RATs remains to today, their use has evolved. In the last decade more and more RATs were used in espionage, financial and state sponsored attacks [3]–[5]. While many of them had their source code leaked or open sourced, the market for Fully Undetectable (FUD) RATs and special plugins matured. Nowadays, RATs have become a commodity.

Despite the abundance of reports on individual RAT families and attacks that use them [6], there is no previous research that looks at RATs as a whole. The growth and evolution of RATs appears to have escaped public attention so far. The lack of a more generalist research hinders the understanding and development of new techniques and methods to better detect them.

This paper aims to start a discussion on RATs as a unique phenomenon that requires further study. We argue that in the last 10 years a shift has occurred in the threat landscape where RATs have become a commodity. This work analyzes the growth of Remote Access Trojans, describes their key technological elements, their functionality, and analyzes how they propagate. Furthermore, this work presents a timeline of the last 30 years of RATs evolution, a detailed overview of the most well-known RATs during 2019-2020, and an analysis of how they have been commercialized.

The main question this research explores is, are Remote Access Trojans a commodity in the underground? Answering this question, the contributions of this paper are:

- The first and most comprehensive timeline of the last 30 years of RATs.
- An overview of the commoditization of the most well-known RATs in 2019-2020.
- A first analysis on the types of attacks and attackers using RATs.

2. Methodology

To address the analysis of RATs we first searched and methodologically analyzed a comprehensive list of Remote Access Trojans since their first public appearance in 1996 until 2018. These RATs, shown in the timeline of Figure 1, were found from public sources and inquiries with the community, and are the base tools analyzed in this work.

DOI 10.1109/EuroS&PW51379.2020.00066

The years 2019 and 2020 were not included in this research as the information available for this time is at the moment not comprehensive and incomplete.

We chose a small subset of RATs in order to study their specific characteristics, their users and how they are commercialized. These RATs were selected using the following methodology. First, we searched on well-known forums for RATs that users were *talking* about or *recommending* to each other in the period from January 2019 to March 2020. We consulted HackForums [7], Sinister.ly [8], and Nulled [9]. Second, taking as an input the list of RATs created in the previous step, we searched for those RATs in websites that were selling hacking tools, software, and other goods. Third, we limited the scope of RATs to those that were being sold in two or more of the above mentioned marketplaces. Fourth, we assembled the final list of RATs to study: WebMonitor RAT, Android Voyager RAT, Remcos RAT, SpyNote RAT, Luminosity Link RAT, Omni Android RAT, Ozone RAT, Imminent Monitor RAT, NanoCore RAT, NetWire RAT and CyberGate RAT. Fifth, further information was collected from public intelligence sources such as blogs, news articles and forums on each of the selected RAT.

3. Overview of Remote Access Trojans

In order to define a common ground to further the understanding of RATs, we first introduce some of the key technical elements of every Remote Access Trojan. Then we present a timeline showing the growth of RATs over the last 30 years. Finally we discuss common functionality found among RATs.

3.1. Key Technical Elements

Remote Access Trojans have two key elements: *client* and *server*. Additional RATs components include the *builder*, *plugins* and *crypter*. A RAT server is the program installed on the victim's device. The server is configured to connect back to the attacker. The client is the program used by the attacker to monitor and control infected victims: it allows the visualization of all active victims infections, displays general information about each infection, and allows to manually perform individual actions on each victim.

The builder is a program that allows to create new RAT servers with different configurations. When attackers move infrastructure quickly, launch new attacks, and require flexibility, builders save time and provide agility.

RATs come with certain fixed functionality. To add more capabilities, some RATs rely on plugins. Not all RATs offer this capability, however the most used ones do, and good plugins are craved by the cybercrime community. These plugins are one of the main differentiators in terms of cost in the underground market.

To be more efficient and hard to detect, attackers use crypters to make the RAT servers Fully Undetectable (FUD). Crypters are programs that take a given program, read the code, encrypt it with a key, and automatically create a new program that contains the encrypted code and key to decrypt it. Upon execution the key will be used to automatically decrypt the original program. Crypters are used to avoid detection by anti-virus engines.

3.2. Thirty Years Timeline of RATs

To better understand the growth and evolution of RATs, it was necessary to investigate and build a corpus of the most well-known Remote Access Trojans in history that had the key technical elements described previously. We were able to find, reference and document many RATs since 1996 to 2018 by looking at reports, code, and forums. These RATs were also grouped in families, with slight variations of the same RATs grouped together. The final list contains 337 unique families of RATs, registering the first time seen, or date of the first public report about them.

The collected information was used to build the first and most comprehensive timeline of RATs to date. The timeline is illustrated in Figure 1, and it is divided in three phases shown in the figure as different dotted lines. The first phase is from 1990 to 1999; the second phase is from 2000 to 2009; and the third phase is from 2010 to 2018. In Figure 1 we also highlight in bold pink color the 11 RATs that will be analyzed in more detail in the following sections.

The oldest RAT was first developed in 1996 [10], however legitimate Remote Access Tools were first created in 1989 [11]. Since then, the number of RATs has grown rapidly. Figure 1 illustrates 337 of the most well-known RAT families during 1996–2018. The first period, 1996-1999, was marked by home-made RATs. In these years, everyone made their own RAT, however these did not prosper nor were heavily used. Among the most prominent ones were Back Orifice, Sub7 and Netbus, which together defined a generation by being innovative and disruptive. The second period, 2000-2009, showed a slight growth of more mature RATs, that were intended for fun but were started to be used for attacks and profit. Among the highlights of this period are Gh0st, PoisonIvy and DarkComet. The third period, 2010-2018, showed an important shift. RATs became a commodity. The market matured, RAT sellers were expected to provide support, new features, and in some cases even to host part of the infrastructure.

The growth of RATs in the last decade depends on a combination of multiple factors. The maturity of the cybercrime ecosystem, the specialization of work in the underground communities, and interdependence of threat actors are some of the key factors that led to an increase in the demand of new and better malicious software, and RATs among them. To understand the real cause however, a more extended analysis and study is needed.

3.3. Functionality

The server-side functionality offered by each RAT will vary depending on the targeted platform and the intent for which the RAT was created. There is not standardized set of features among RATs, however certain features are expected, namely:

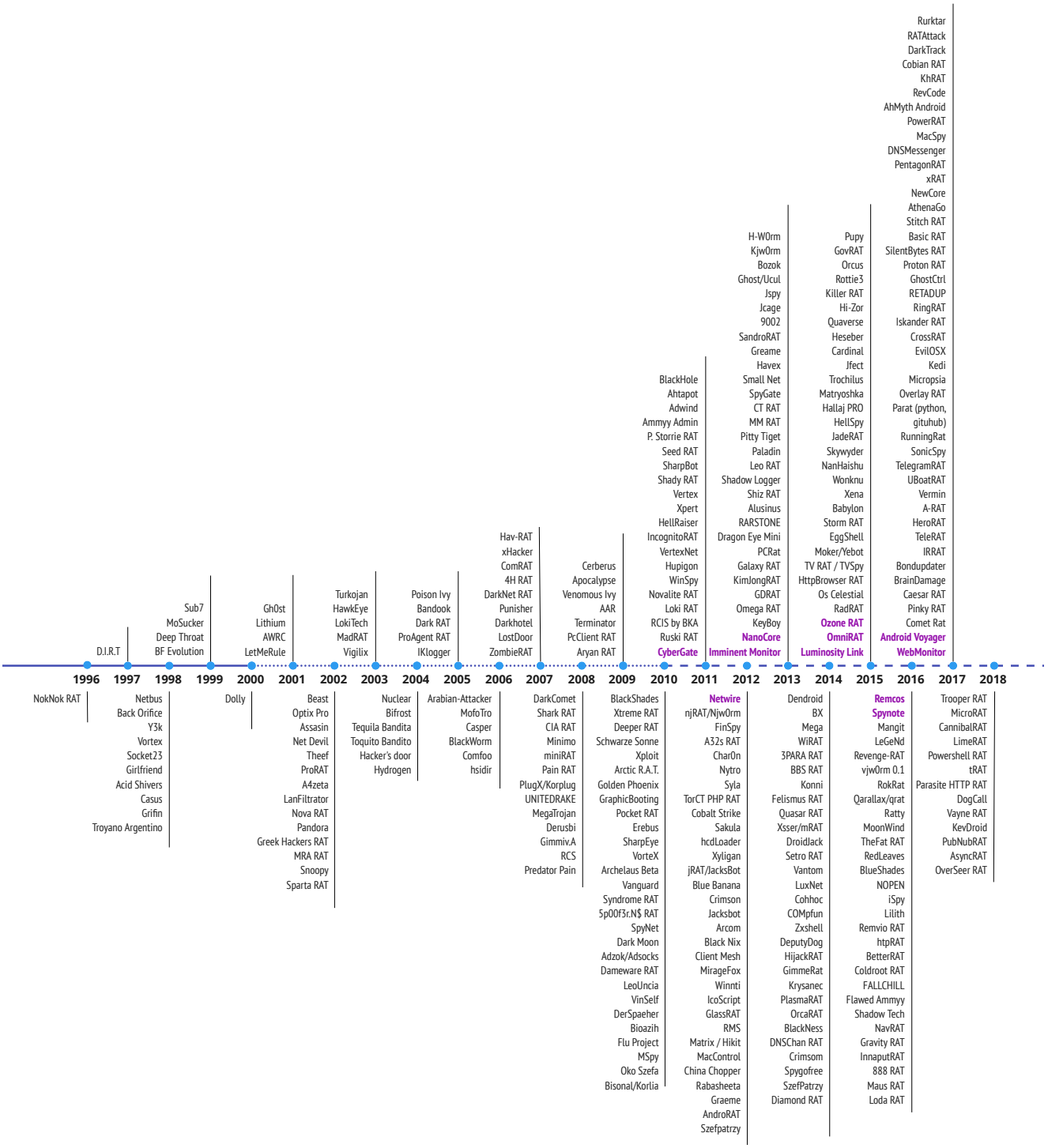

Figure 1. Timeline of 337 well-known Remote Access Trojans families during 1996-2018, ordered by year of first seen or reported by the community. The timeline is divided in three phases marked by dotted lines. The last phase clearly shows a significant growth compared with the previous phases. In bold pink we highlight the 11 RATs this research focuses on.

- Webcam: take screenshots or full video recording through the victim's webcam.
- Microphone: access the microphone to record audio.
- Display: take screenshots or full screen recording of the victim's desktop.
- Keylogger: capture keystrokes from the victim.
- System: perform system operations such as retrieving system information, file management, hard drive and RAM access, installing programs, and other.
- Peripherals: access to peripherals devices including Bluetooth, CD/DVD reader, and others.

The quality of the RATs however does not only depend on the server side functionality. On the client-side, the following factors are considered important:

- Stealthiness: the more stealth and hard to detect the RAT is, the better.
- Stability: server and client stability are paramount qualities of a successful RAT.
- Graphical interface: the more user friendly the client control panel, the better.
- Encryption: traffic encryption is very important to hide the content in the network.
- Dependencies: the fewer dependencies needed for a RAT to work, the better.

3.4. Propagation Methods

The distribution and propagation of Remote Access Trojans rely heavily on social engineering. Social engineering refers to the psychological manipulation of humans into acting in a desired way, usually with the aim of obtaining information or in this case, installing a malicious program.

Traditional phishing and spear phishing campaigns are the preferred method to distribute RATs using malicious attachments [12]–[15]. Some Facebook pages were also known for luring users to install RATs [16]. These pages contain links to download what looked like normal software, which in reality would download RATs. Channels in secure messengers such as Telegram and WhatsApp were also known to spread malicious links that would lead to RATs [17], [18].

4. Commoditization of RATs

Just like other types of malware, RATs are openly commercialized. This section provides insights on eleven selected RATs that were more recommended by users in forums during 2019-2020. This section will focus on their characteristics, special features, and provide insights of their commercialization on different marketplaces.

Based on the analysis of the market it is possible to say that far from being custom-made unique tools, RATs have become a commodity. They have become a group of standardized products that are not very different from each other. The variation of prices is not given by the functionality of the RATs per se, but instead by the sellers themselves being able to offer additional services, extended functionality or technical support. No matter the skill level, attackers are able to chose from a wide range of very affordable options and adjust their attack to the final product selected. Most RATs do not have a huge technological advantage, but better reviews, recommendations and in the end, better marketing.

4.1. Overview of the Eleven Selected RATs

The selected RATs, as summarized in Table 1, are WebMonitor RAT, Android Voyager RAT, Remcos RAT, SpyNote RAT, Luminosity Link RAT, Omni Android RAT, Ozone-RAT, Imminent Monitor RAT, NanoCore RAT, NetWire RAT and CyberGate RAT. These RATs are also highlighted on Figure 1 in bold pink color.

CyberGate RAT was first seen in 2011 [19]. The client is written in Delphi, the server is believed to be written in C++ and is very lightweight, 40 KB uncompressed. It seems to share part of its code with an earlier RAT known as Xtreme RAT from 2010, whose source code was leaked [20]. This RAT targets specifically Windows machines, both 32Bit and 64Bit. Its key functionalities include keylogger, screenshot logger, password recovery and microphone capture.

NetWire RAT was first seen in 2012 [21] and is multi-platform, being able to target not only Windows machines, but also Mac, Linux and Android. Both client and server are written in C. It offers full remote access with traditional functionalities such as keylogger, system management, password recovery and others. It allows heavy customization.

Imminent Monitor RAT, also known as IM-RAT, was first seen in 2012 [22]. It targets Windows machines, and both client and server are written in .NET. Imminent Monitor was commercialized as a benign administration tool, however researchers confirmed that some of its functionalities made the RAT undetectable for the victim, including recording from the webcam undetected by turning off the webcam light [23]. A version of Imminent Monitor allowed attackers to run a cryptocurrency miner on the infected machine.

NanoCore RAT was first publicly seen in 2013, while its author started coding it on late 2012 [24]. Bot client and server are written in .NET. The source code of NanoCore has been leaked multiple times, and while the original author was arrested there are versions of it still being sold today. NanoCore was reported to be used for state-sponsored attacks [3]. Among its features it offers a plugin system to extend its functionality, remote chat, and uPnP support.

Luminosity Link was first seen in 2015 [25], targets Windows machines and both client and server are written in .NET. The source code was leaked, however it is still being sold even though the author was arrested [26].

Omni Android RAT, also known as OmniRAT, was first seen in 2015 [27]. This RAT is multi-platform, allowing to target Windows, Mac, Linux and Android victims. For Android devices it allows to retrieve a high number of information, including battery level, widgets installed, Bluetooth, calls, and many others.

TABLE 1. TECHNICAL OVERVIEW OF ELEVEN OF THE MOST COMMON RATS DURING 2019-2020

RAT	First Seen	Targeted Platform	Used in targeted attacks	Client Source Code Language	Server Source Code Language
CyberGate RAT	2011	Windows	Yes	Delphi	C++
NetWire RAT	2012	Windows, Mac, Linux & Android	Yes	C	C
Imminent Monitor RAT	2012	Windows	Yes	.NET	.NET
NanoCore RAT	2013	Windows	Yes	.NET	.NET
Luminosity Link RAT	2015	Windows	Yes	.NET	.NET
Omni Android RAT	2015	Windows, Mac, Linux & Android	Yes	Java	Java
Ozone RAT	2015	Windows	Yes	C++	C++
Remcos RAT	2016	Windows	Yes	C++	C++
SpyNote RAT	2016	Android	Unknown	Visual Basic	Java
Android Voyager RAT	2017	Android	Unknown	Java	Java
WebMonitor RAT	2017	Windows, Linux, Mac & Google OS	Unknown	C++	C++

Ozone-RAT was created in 2015 [28]. Both client and server are written in C++, and it targets specifically Windows machines. It offers traditional functionalities such as remote desktop, keylogger and system management. One of the main highlights of this RAT is that it offers a hidden VNC functionality.

Remcos RAT was first seen in 2016 [29]. Both client and server are written in C++ making it lightweight. Remcos targets 32Bit and 64Bit Windows machines. Its functionality includes uploading and downloading files, system management, and keylogger. There are several variants observed in the wild, which suggest that the source code may have been leaked.

SpyNote RAT version 2 was first seen in 2016 [30], however it may have been created earlier. The client is written in Visual Basic, and the server in Java. It targets Android devices. Among its functionality it includes the ability to access contacts, listen to calls, access front and back cameras, read SMS, and system management without requiring root access. The builder of SpyNote was leaked [31] and thus, multiple versions have been observed of this RAT.

Android Voyager RAT, also known as Voyager RAT, was first seen in 2017 [32]. Both client and server are written in Java, and its author claims to be original and not based from other leaked RAT. It targets Android devices. The functionality offered depends on whether there is root access on the device or not. Among the novel features, it claims that with root access it can survive factory reset on the Android device.

WebMonitor RAT was first seen in 2017 [33]. Both client and server are written in C++. WebMonitor targets Windows, Linux, Mac and Google OS. It's designed to be an *enterprise* class RAT able to compete with TeamViewer and other commercial remote access software. It offers stability, full remote control, and the management of clients through a web page being multi-platform on the client side as well.

4.1.1. RAT Features. In terms of functionality, all the selected RATs provide the same basic features as described in Section 3.3. These features however are complemented by additional features that characterize and differentiate RATs among each other. However until today, there is not a common standardization of features to compare RATs. For instance, for the CyberGate RAT we could find more than 70 individual features [34], while for NetWire the user manual only lists a few dozen [35]. While at first sight CyberGate seems to have more features, that is not the case. The only difference is that the features described for CyberGate are more detailed than those for NetWire, making a comparison a difficult task.

4.2. Marketplaces

Just like other malware, RATs are openly commercialized through forums and marketplaces. In this paper we focus on six marketplaces selling RATs among other hacking tools and services. The selected marketplaces are shown on Table 2, along with a summary of the RATs offered in each market and their prices.

Although the majority of well-known RATs are open-source or had their code leaked, sellers commercialize RAT packages. These include the fully undetectable RAT with plugins and its builder. Sellers may sell the RAT once, or may offer subscriptions for a limited time. Subscriptions are sold in tiers, such as Basic, Premium and Pro, or Startup, Small Business and Enterprise. When sold via subscriptions, the offerings vary according to the number of simultaneous clients, functionality, number of plugins included, and concurrent tasks executed.

DaVinciCoders (codevinci.pw) is a website that sells Microsoft Office exploits, crypters, keyloggers, RATs and botnets. It has four RATs for sale: Imminent Monitor, NanoCore, Luminosity Link, and Ozone RAT. It offers plugins and support. This market sells the RAT, without licensing, thus having lower prices than other markets. The payment is handled via rocketr.net, however at the time of writing, the site has banned the products due to violations of their terms of services.

Secret Hacker Society (secrethackersociety.com) is a website that sells exploits, botnets, RATs, keyloggers, crypters, tutorials and hardware devices. It has nine RATs for sale with prices ranging from 55 USD to 200 USD. Some RATs are offered through licensing and special FUD features, leading to higher prices than other markets. Payments are handled via perfectmoney.is or Bitcoin.

TABLE 2. COMMERCIALIZED PRICES OF RATS IN ONLINE MARKETPLACES

RATs	Sellers and Marketplaces (USD)					
	DaVinciCoders	Secret Hacker Society	buyallrat588	Dorian Docs	FUD Exploits	Ultra Hacks
CyberGate RAT	-	200	30-65	-	-	-
NetWire RAT	-	120	-	-	120	180
Imminent Monitor RAT	45	-	50-120	20-70	20-100	-
NanoCore RAT	45	96	-	-	150-170	-
Luminosity Link RAT	75	55	-	-	150	-
Omni Android RAT	-	80	60-150	120	120	180
Ozone RAT	75	-	-	-	170	-
Remcos RAT	-	99	-	-	170	-
SpyNote RAT	-	69	80-140	-	150-170	69
Android Voyager RAT	-	90	30-65	30-150	30	55-250
WebMonitor RAT	-	-	-	60-120	60	70-140

Buy All Rat (buyallrat588.com) is a website that sells hacking software, RATs, Exploits, Spoofers, Private Mailers, SMTP, Bot Nets, crypters, Shells, VPNs, keyloggers and other. It has five RATs on sale on two tiers: Basic and Pro. Pro licenses are more expensive as their include typically lifetime access, technical support, one week money back guarantee, and more than one device licensing. The seller doesn't perform direct sales, customers need to send an email request and all exchange is done privately.

Dorian Docs (doriandocs.com) is a website that sells accounts, RATs, fake IDs and fake documents. It has four RATs on sale and each RAT has a different tier: single price, Business/Professional, Startup/Small Business/Business, 1 month/3 months/6 months/Lifetime. Payments are made with cryptocurrency, accepting Bitcoin, Monero, Ethereum and Litecoin.

FUD Exploits (fudexploits.com) is a website that sells botnets, crypters, passports, RATs, and other products. It has ten RATs on sale, and it offers different RAT packages at different prices, varying on versions, number of plugins, and support. Payments are made using Bitcoin.

Ultra Hacks (ultrahacks.org) is a website that sells tutorials, RATs, botnets, hardware, and services. It has five RATs on sale, only two of them are offered in two tiers Professional/Premium, the rest is offered in a single option. The seller accepts payments in Bitcoin, Monero, Litecoin, direct by transfer SEPA, cash on delivery and Perfect Money.

The variation in price depends on the how fully undetectable the RAT is and on the type of license purchased, if any. In terms of detection, a RAT can be detectable, fully undetectable at runtime, fully undetectable at scan time (AV scans), or both. The price will also depend on the type of license. Markets such as DaVinciCoders sell just the RAT without any type of license, leading to lower prices. Markets such as FUD Exploits sell the license to use the RAT for a number of devices, typically 1 device. Licenses can be for a finite time, or infinite, leading also to higher prices.

5. Characterizing Attacks

To better understand the market and context of these RATs, this section provides a first analysis of different known types of attacks done with RATs and the different sectors or type of crimes they focus on. In contrast with botnets, RATs are precision tools that excel in targeted attacks meant to extract specific information from victims. RAT attacks differ from most malware attacks in several aspects. First, contrary to botnets where an attacker controls all the bots simultaneously, attackers control each RAT infection manually. Second, due to this individual control of each victim, the sequence of actions on the victims may never be the same in two infections. Third, the number of simultaneous infections that an attacker can control are limited by the skill of the attacker. No attacker will be able to control half a million victims as with botnets.

5.1. Business Email Compromise

Business Email Compromise (BEC) is a type of scam directed at companies or organizations that pay their suppliers via wire transfers [36]. In BEC attacks, attackers use different techniques with the aim of redirecting the transfer of funds to attackers' accounts instead of the legitimate ones, thus stealing the money. While traditionally information stealers were the preferred tool in BEC attacks, there has been a shift and nowadays the use of RATs is becoming the norm [37].

5.2. Espionage

RATs are designed for spying on victims, and cyber espionage is the type of attack where they excel at. Cyber espionage attackers may develop their own RATs [38], [39], or use well-known commercial RATs for their operations. Advanced attackers, like the Tonto APT group, has been known to use the same self-developed RAT for over a decade [40]. There are pros and cons of using well-known RATs for a highly confidential operation. Using well-known RATs may leave unnecessary tracks that could lead to identify the attacker, and the RAT may not have all the needed functionality. Additionally, commercially available RATs may not provide enough stability or the stealthiness required for cyber espionage activities. However, developing a custom-made RAT can clearly help identify the attacking group very easily and help in attribution.

5.3. Targeted Attacks

Targeted attacks are attacks that are carefully planned, target a very narrow set of victims, and have often a specific goal. RATs are widely used in this type of attacks. From the eleven RATs mentioned in the previous section, 9 of them were used in targeted attacks [41] [42] [43] [44] [45] [46] [47] [48] [49]. The majority of the reports on RATs used on targeted attacks focus on the delivery method and not on how the malware was used. It is generally understood that RATs are mainly used to monitor the infected device, steal documents, and steal credentials that can be used to move laterally on the compromised organization.

6. Characterizing Attackers

RAT users are not homogeneous. They can be separated in three groups according to their aim: (i) users that use RATs for educational purposes, fun or pranks, (ii) for advanced attacks and espionage activities, and (iii) for cybercrime (whether selling RATs to other actors or buying RATs for attacking).

6.1. Educational Purposes

Attackers using RATs for educational purposes, fun or pranks rarely purchase commercial RATs. They will likely write their own or modify existing ones. The renowned development platform GitHub [50] contains dozens or hundreds self-made RATs created and shared publicly with the disclaimer of being for *education purposes only*. In underground forums, the hacker community still believes that real hackers will create their own RAT, which incentives this activity.

6.2. Advanced Attacks

State sponsored attackers and cyber crime organizations are believed to create their own tools customized to their own needs. An exemplary case in this category is the Tonto APT Group that developed their own RAT and used it for more than a decade [40]. The use of open source tools however may be useful in some scenarios to give false flags or as a distraction.

6.3. Cybercrime

Traditional cybercrime groups are the ones engaged in commercializing RATs. Sellers will use available RATs, modify or enhance them, package them and sell them. They will offer technical support, tutorials, and hosting services. Buyers do not want to get absorbed in technical details and programming, they look to focus on the attacks. Buyers rely on sellers to provide stable tools, with support, and ability to develop further modules for them in case they need them.

7. Conclusion

We have presented a first overview of the growth of Remote Access Trojans by visualizing the 337 most well-known families during 1996-2018. This generalist overview provides an understanding of how this type of malicious software has grown over the last three decades. Insights on eleven of the most prominent RATs during 2019-2020 regarding their commercialization in online marketplaces showed that RATs are technologically not so different from each other. The main differences are in prices due to the added features or additional services offered by the sellers themselves. While it is still believed that real hackers will create their own RAT, business oriented cybercriminals will look for stability, simplicity, support, and guarantee; thus buying RATs instead of crafting their own. These commercial characteristics of RATs mark them as a commodity. Shifts in cybercriminal activities continue to happen and RATs are used more and more in all type of attacks. Their continual growth challenges current detection methods and asks for further research that focuses on RATs as a general malware class and not only in individual RAT families.

Acknowledgment

The authors would like to thank the Czech Technical University for its support. The authors would also like to thank all the individual researchers that shared information and helped during the last three years in building the RAT timeline.

References

[1] *TeamViewer: remote access, remote control and remote support solution*, TeamViewer Germany GmbH. [Online]. Available: https://www.teamviewer.com/

[2] *Ammyy Admin: Remote Desktop Software and Remote Desktop Connection*, Ammyy, Inc. [Online]. Available: http://www.ammyy.com/

[3] E. Kovacs, "Nation-State Actors Use Fileless Tricks to Deliver RATs," 2016. [Online]. Available: https://www.securityweek.com/nation-state-actors-use-fileless-tricks-deliver-rats

[4] W. R. Marczak, J. Scott-Railton, M. Marquis-Boire, and V. Paxson, "When governments hack opponents: A look at actors and technology," *Proceedings of the 23rd USENIX Security Symposium*, pp. 511–525, 2014.

[5] K. J. Higgins, "Schneider Electric: TRITON/TRISIS Attack Used 0-Day Flaw in its Safety Controller System, and a RAT," 2018. [Online]. Available: https://www.darkreading.com/vulnerabilities---threats/schneider-electric-triton-trisis-attack-used-0-day-flaw-in-its-safety-controller-system-and-a-rat/d/d-id/1330845

[6] M. Rezaeirad, B. Farinholt, H. Dharmdasani, P. Pearce, K. Levchenko, and D. McCoy, "Schrödinger's RAT: Profiling the stakeholders in the remote access trojan ecosystem," in *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 1043–1060. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/rezaeirad

[7] *HackForums*, accessed on March 5, 2020. [Online]. Available: https://www.hackforums.net/

[8] *Sinesterly Forum*, accessed on March 5, 2020. [Online]. Available: https://sinister.ly/

[9] *Nulled Forum*, accessed on March 5, 2020. [Online]. Available: https://www.nulled.to/

[10] MegaSecurity, *NokNok 5.0*, accessed via Internet Archive. [Online]. Available: https://web.archive.org/web/20081201090344/http://www.megasecurity.org/trojans/n/noknok/Noknok5.0.html

[11] N. House, *NetSupport Manager - Multi-Platform Remote Control software*, accessed on March 6, 2020. [Online]. Available: http://www.netsupportmanager.com/

[12] X. Zhang, *NetWire Being Spread via Phishing Email*, accessed on March 6, 2020. [Online]. Available: https://www.fortinet.com/blog/threat-research/new-netwire-rat-variant-spread-by-phishing.html

[13] S. Gatlan, *Phishing Campaign Delivers Quasar RAT Payloads via Fake Resumes*, accessed on March 6, 2020. [Online]. Available: https://www.bleepingcomputer.com/news/security/phishing-campaign-delivers-quasar-rat-payloads-via-fake-resumes/

[14] Kaspersky Lab, "Chinese-speaking apt actor caught spying on pharmaceutical organizations," accessed on March 6, 2020. [Online]. Available: https://www.kaspersky.com/about/press-releases/2018_chinese-speaking-apt-actor-caught-spying-on-pharmaceutical-organizations

[15] Cyware, "Adwind rat: An insight into the remote access trojan's malicious activities," accessed on March 6, 2020. [Online]. Available: https://cyware.com/news/adwind-rat-an-insight-into-the-remote-access-trojans-malicious-activities-965b128f

[16] Check Point Research, *Operation Tripoli*, accessed on March 6, 2020. [Online]. Available: https://research.checkpoint.com/2019/operation-tripoli/

[17] Kaspersky GReAT, "Fully equipped spying android rat from brazil: Brata," accessed on March 6, 2020. [Online]. Available: https://securelist.com/spying-android-rat-from-brazil-brata/92775/

[18] B. N, "Hackers launching macos malware via fake whatsapp l website," accessed on March 6, 2020. [Online]. Available: https://gbhackers.com/hackers-launching-unique-macos-malware/

[19] W. Ali, "Cybergate rat - hacking facebook, twitter and email id's passwords," accessed on March 6, 2020. [Online]. Available: http://www.hackersthirst.com/2011/03/cybergate-rat-hacking-facebook-twitter.html

[20] J. T. B. Nart Villeneuve, "Xtremerat: Nuisance or threat?" accessed on March 6, 2020. [Online]. Available: https://www.fireeye.com/blog/threat-research/2014/02/xtremerat-nuisance-or-threat.html

[21] MalwareMustDie, "Mmd-0031-2015 - what is netwire (multi platform) rat?" accessed on March 6, 2020. [Online]. Available: https://blog.malwaremustdie.org/2015/04/mmd-0031-2015-what-is-netwire-rat.html

[22] T. Seals, "Authorities break up imminent monitor spyware organization," accessed on March 6, 2020. [Online]. Available: https://threatpost.com/authorities-imminent-monitor-spyware-organization/150731/

[23] Palo Alto Unit42, "Imminent monitor – a rat down under," accessed on March 6, 2020. [Online]. Available: https://unit42.paloaltonetworks.com/imminent-monitor-a-rat-down-under/

[24] K. Poulsen, "Fbi arrests hacker who hacked no one," accessed on March 6, 2020. [Online]. Available: https://www.thedailybeast.com/fbi-arrests-hacker-who-hacked-no-one

[25] J. Grunzweig, "Investigating the luminositylink remote access trojan configuration," accessed on March 6, 2020. [Online]. Available: https://unit42.paloaltonetworks.com/unit42-investigating-the-luminositylink-remote-access-trojan-configuration/

[26] B. Krebs, "'luminositylink rat' author pleads guilty," accessed on March 6, 2020. [Online]. Available: https://krebsonsecurity.com/2018/07/luminositylink-rat-author-pleads-guilty/

[27] N. Chrysaidos, "Droidjack isn't the only spying software out there: Avast discovers omnirat," accessed on March 6, 2020. [Online]. Available: https://blog.avast.com/2015/11/05/droidjack-isnt-the-only-spying-software-out-there-avast-discovers-that-omnirat-is-currently-being-used-and-spread-by-criminals-to-gain-full-remote-co

[28] "Honest ozone rat review," accessed on March 6, 2020. [Online]. Available: https://raidforums.com/Thread-Honest-Ozone-Rat-Review

[29] A. Hinchliffe, "Emea bi-monthly threat reports: Turkey, saudi arabia & united arab emirates," accessed on March 6, 2020. [Online]. Available: https://unit42.paloaltonetworks.com/unit42-emea-bi-monthly-threat-reports-turkey-saudi-arabia-united-arab-emirates/

[30] "Spynote [android rat] v2.3 server setting," accessed on March 7, 2020. [Online]. Available: https://www.youtube.com/watch?v=voeLG1H6qSY

[31] J. Soo, "Spynote android trojan builder leaked," accessed on March 7, 2020. [Online]. Available: https://unit42.paloaltonetworks.com/unit42-spynote-android-trojan-builder-leaked/

[32] "Voyager rat," accessed on March 6, 2020. [Online]. Available: https://hackforums.net/showthread.php?tid=5723439

[33] "Webmonitor pc [#1 rat on the market, c++/native (no .net), no portforward, keylogger]," accessed on March 6, 2020. [Online]. Available: https://hackforums.net/showthread.php?tid=5621975&highlight=Webmonitor

[34] *CyberGate RAT COMPLETE TUTORIAL*, accessed on May 31, 2020. [Online]. Available: https://atjeh-vb6.blogspot.com/2013/05/cybergate-rat-complete-tutorial.html

[35] *NetWire Product Overview*, accessed on May 31, 2020. [Online]. Available: https://www.worldwiredlabs.com/documents/NetWire%20User%20Manual.pdf

[36] "Business email compromise (bec)," accessed on March 7, 2020. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)

[37] I. Ilascu, *Nigerian BEC Scammers Shifting to RATs As Tool of Choice*, accessed on March 7, 2020. [Online]. Available: https://www.bleepingcomputer.com/news/security/nigerian-bec-scammers-shifting-to-rats-as-tool-of-choice/

[38] K. Zykov, *Hello! My name is Dtrack*, accessed on March 7, 2020. [Online]. Available: https://securelist.com/my-name-is-dtrack/93338/

[39] J. Miller-Osborn and M. Harbison, *Rancor: Cyber Espionage Group Uses New Custom Malware to Attack Southeast Asia*, accessed on March 7, 2020. [Online]. Available: https://unit42.paloaltonetworks.com/rancor-cyber-espionage-group-uses-new-custom-malware-to-attack-southeast-asia/

[40] P. R. Warren Mercer and V. Ventura, *Bisonal: 10 years of play*, accessed on March 7, 2020. [Online]. Available: https://blog.talosintelligence.com/2020/03/bisonal-10-years-of-play.html

[41] M. Mimoso, *AutoIt Used in Targeted Attacks to Move RATs*, accessed on March 7, 2020. [Online]. Available: https://threatpost.com/autoit-used-in-targeted-attacks-to-move-rats/114406/4/

[42] *Netwire RAT Behind Recent Targeted Attacks*, accessed on March 7, 2020. [Online]. Available: https://www.kashifali.ca/2015/03/02/netwire-rat-behind-recent-targeted-attacks/

[43] C. Cimpanu, *Authorities take down 'Imminent Monitor' RAT malware operation*, accessed on March 7, 2020. [Online]. Available: https://www.zdnet.com/article/authorities-take-down-imminent-monitor-rat-malware-operation/

[44] M. Baezner, *Regional rivalry between India-Pakistan: tit-for-tat in cyberspace*, accessed on March 7, 2020. [Online]. Available: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-04.pdf

[45] M. Kumar, *Exclusive: German Police Raid OmniRAT Developer and Seize Digital Assets*, accessed on March 7, 2020. [Online]. Available: https://thehackernews.com/2019/06/police-raid-omnirat-developer.html

[46] F. B. Jr. and J. Salvio, *German Speakers Targeted by SPAM Leading to Ozone RATFloser Bacurio Jr. and Joie Salvio*, accessed on March 7, 2020. [Online]. Available: https://www.fortinet.com/blog/threat-research/german-speakers-targeted-by-spam-leading-to-ozone-rat.html

[47] *Remcos RAT Abuses Office Vulnerabilities to Target Businesses*, accessed on March 7, 2020. [Online]. Available: https://www.enigmasoftware.com/remcos-rat-abuses-office-vulnerabilities-target-businesses/

[48] R. Abel, *Spynote RAT posing as Netflix plus other popular apps*, accessed on March 7, 2020. [Online]. Available: https://www.scmagazine.com/home/security-news/cybercrime/spynote-rat-posing-as-netflix-plus-other-popular-apps/

[49] S. Desai, *SpyNote RAT posing as Netflix app*, accessed on March 7, 2020. [Online]. Available: https://www.zscaler.com/blogs/research/spynote-rat-posing-netflix-app

[50] "Github development platform." [Online]. Available: https://github.com/