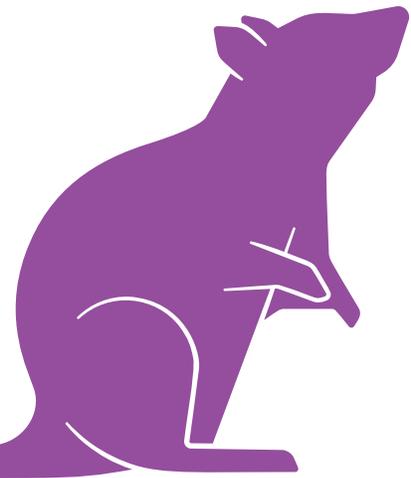


# THE GATEWAY TROJAN

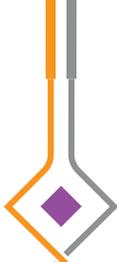


Volume 1, Version 1

# TABLE OF CONTENTS

|  |    |
|--|----|
| <b>About This Report</b> .....               | 1  |
| <b>Why This Malware?</b> .....               | 2  |
| <b>The Basic Questions About RATs</b> .....  | 2  |
| <b>Different Breeds of RATs</b> .....        | 5  |
| Symantec's Haley Subcategories of RATs ..... | 6  |
| <b>Dissecting a RAT</b> .....                | 7  |
| <b>Category II: Common RATs</b> .....        | 9  |
| Back Orifice.....                            | 9  |
| Bifrost.....                                 | 10 |
| Blackshades.....                             | 11 |
| DarkTrack .....                              | 13 |
| Gh0stRat .....                               | 14 |
| NanoCore RAT .....                           | 15 |
| njRAT .....                                  | 17 |
| Poison Ivy.....                              | 18 |
| Sub7.....                                    | 19 |
| Xtreme RAT.....                              | 20 |
| <b>Mobile RATS</b> .....                     | 21 |
| Adwind-UNRECOM .....                         | 22 |
| AndroRAT.....                                | 23 |
| <b>Uncommon RATS</b> .....                   | 24 |
| <b>Category III: Criminal Tools</b> .....    | 25 |
| Carbanak RAT.....                            | 25 |
| Dyreza/Dyre.....                             | 27 |
| How Dyre Works .....                         | 28 |
| Kraken RAT .....                             | 29 |
| Sir DoOom .....                              | 30 |





# TABLE OF CONTENTS

|   |    |
|---|----|
| <b>Category IV: Nation State Tools</b> .....          | 31 |
| Explosive .....                                       | 31 |
| Regin.....  | 33 |
| Trojan Laziok .....                                   | 34 |
| <b>Popular Places for RATs</b> .....                  | 35 |
| <b>Summary</b> .....                                  | 38 |
| <b>Appendix A: Known Anti-Virus Identifiers</b> ..... | 39 |
| Category II Identifiers .....                         | 40 |
| Category III Identifiers.....                         | 41 |
| Category IV Identifiers.....                          | 42 |
| <b>Acknowledgments</b> .....                          | 45 |



EACH SCREENSHOT OF YOUTUBE PAGES AND WEBSITES WAS GRABBED DURING DIGITAL CITIZENS RESEARCH AND MAY NOT REFLECT THE CURRENT STATUS OF ANY PAGE.



## ABOUT THIS REPORT

In our first report on Remote Access Trojans (RATs), the Digital Citizens Alliance showed how unethical computer hackers are increasingly using this malware to target consumers in 1:1 attacks. That report, [Selling “Slaving”](#), followed the subset of hackers known as “ratters” to see how they spread this dangerous code to devices around the world. We saw how ratters used YouTube and content theft sites as tools to spread their malware and celebrate their disturbing activities.

We also found that RATs are cheap, easy to get, and easy-to-use tools that can teach wannabes the basics of hacking. A wannabe who stays below radar, i.e., who refrains from becoming violent, exploiting teens, or going after crazy amounts of money can hack devices halfway around the world before cyber sleuths get their virtual machines (VMs) running. Security expert Georgia Weidman, CEO of Bulb Security, began playing with RATs in her lab, “not attacking anyone, just seeing how they worked. I wasn’t sophisticated enough to write my own RATs or write exploits then, but it led me down the path of becoming an ethical hacker, and now I write my own security tools and responsibly disclosed exploits.”

While Weidman is a white hat hacker working to

protect people from RATs, her story and others we heard made us wonder if RATs could be to malware what some argue marijuana is to drug use: a “gateway” that could lead to dark, dangerous digital activities. During our research and conversations with cyber security experts, we began to refer to RATs as “The Gateway Trojan” because of their lure for novices. While some like Weidman do good work, others use their skills to put regular people in great danger. As a society, we can no longer simply dismiss them as a problem too complicated to understand, or one that only those fluent in coding can tackle. We need increased public awareness about Remote Access Trojans and black hat hackers that wreak havoc on ordinary citizens.

This report will not make you a cyber security professional. We hope it will help you form questions for professionals if you are concerned that your device has been compromised, or if you know someone who might have gotten caught up in this shadowy world. In other words, we hope you finish this paper with enough knowledge to make you “just dangerous enough” to help stop a ratter from hacking someone important to you.

<sup>1</sup> A virtual machine is a software emulation of a standard PC. A virtual system allows a single hardware platform to run multiple workstations or servers. These VMs are preferred by security professional because if they get infected, these VMs can be deleted and a new clean server can be created from a master copy.

**A WARNING TO CONSUMERS** - Digital Citizens researchers used specialized workstations with up-to-date tools and safeguards during their research. We strongly urge you not to try to replicate this research without the right protection and expertise. Clicking on the links seen on many of these YouTube pages and Hack Forums could put you, your device, and your data in the crosshairs of a ratter.



## WHY THIS MALWARE?

Every day, hundreds of thousands of new malicious files are unleashed into the wild. The anti-malware laboratory PandaLabs estimates about 227,000<sup>2</sup> are dropped onto the devices of unsuspecting consumers, while Symantec puts the number closer to 1,300,000.<sup>3</sup> There is no debate that the overwhelming majority of malicious files are some kind of Trojan.

### There are six different kinds of Trojans<sup>4</sup>:

- **Remote Access Trojan**
- **Data Copy/Destruction** (steal data/key logger/data removal/cyberlockers)
- **Downloader** (which downloads other malware)
- **File Server Trojan** (Proxy, FTP, IRC, Email, HTTP/HTTPS, etc.)
- **Security Software Disabler**
- **Distributed Denial-of-Service (DDoS)**

All threaten consumers, but Remote Access Trojans (RATs) are particularly dangerous because they're so easily acquired, deployed, and spread by tech novices.



## THE BASIC QUESTIONS ABOUT RATs

### WHO ARE THESE "RATTERS"?

"Skilled developers call some ratters "script kiddies" because the malware is so popular with wannabe threat actors. Many ratters have some basic knowledge about computer systems, but lack the skill to write their own code or build applications."

Kevin Haley, Director of Product Management for Symantec Security Response, and one of the technical advisors on Symantec's [Internet Security Threat Report \(ISTR\)](#), said in a phone interview with Digital Citizens Alliance, "RATs are easy to use.... You have to figure out how to get it on somebody's machine, but once it's on there, it takes no technical skills to implement."

<sup>2</sup><http://www.pandasecurity.com/mediacenter/src/uploads/2017/02/Pandalabs-2017-Predictions-en.pdf>

<sup>3</sup>[https://www.symantec.com/security\\_response/publications/monthlythreatreport.jsp](https://www.symantec.com/security_response/publications/monthlythreatreport.jsp)

<sup>4</sup>This is a combination of different lists of Trojan horse malware. It comes from <https://blog.malwarebytes.org/intelligence/2013/06/what-are-trojans/> and <http://www.infoniac.com/hi-tech/types-of-trojan-horse-viruses.html> and [http://www.webopedia.com/TERM/T/Trojan\\_horse.html](http://www.webopedia.com/TERM/T/Trojan_horse.html)



When you feel comfortable in your proficiency and are in an environment that allows you to learn and expand, you begin to find potential partners and other people to help you ... do something more sophisticated."

YouTube and the DarkNet, by reading chats on sites like Reddit, and joining community bulletin boards at Hack Forums.

These ratters can learn more about finding and spreading RATs from instructional videos on

The image shows a Google search for "spreading rats" and a screenshot of the top search result, a forum thread on Hack Forums. The search results include:

- How to Spread Bots/Rats - Page 1 - Hack Forums**  
www.hackforums.net › ... › Hacking Tutorials  
Apr 4, 2009 - 10 posts - 10 authors  
Intro ----/--- When it comes too spreading your bot's and your rats, it can be quite easy or challenging for the average retard. What people do not understand is that spreading is very easy depending on the way that you do it. Below, is a FEW methods on how to spread.You visited this page on 6/23/15.
- After 8 centuries, rats exonerated in spread of bubonic plague**  
www.washingtonpost.com/.../after-8-centuries-rats-...  
Feb 24, 2015 - After nearly eight centuries of accusing the black rat as the cause of the bubonic plague, scientists say they have compelling evidence that the disease was actually spread by fleas.
- Great Rat/Keylogger Spreading method!!! No**  
www.youtube.com/watch?v=fOhYhQ...  
Nov 3, 2012 - Uploaded by privateservers  
Great spreading method. ... how to spre [with download link!] - Duration: 10:07. by
- Spreading viruses is easy - YouTube**  
www.youtube.com/watch?v=KKNYuS...  
Sep 13, 2012 - Uploaded by Treesnfleas  
Here is me Wiz khalifa from leakforums.com just wanted 2 show you guys how easy it

The forum thread screenshot shows the title "How to Spread Bots/Rats" and the following text:

Intro  
----/---  
When it comes too spreading your bot's and your rats, it can be quite easy or challenging for the average retard. What people do not understand is that spreading is very easy depending on the way that you do it. Below, is a FEW methods on how to spread.

----/---  
Methods  
----/---  
Torrents: A very common way too spread files over the net  
--  
P2P: A few very good example is Limewire  
--  
IM: If you do this mixed with a bit of SE you have a good chance of infecting the victim  
--  
Warez: If you have a nice account which is trusted, start spreading your RAT  
--  
Personal Site: Upload a few files which are in your sites category binded with your rat  
--  
VIP: If you have VIP on a site, either make a fake tool and bind with your RAT, or leech off another VIP site and share with your binded RAT  
--  
Hacking Sites: Lets say you want too get.. Runescape accounts. Find a autobot or somin And bind your RAT and share on a Runescape hacking site. This way You have more of a chance of getting runescape accounts.



## WHAT CAN A RAT DO TO A DEVICE?

In his paper, [2015: Year of the Rat – Threat Report](#), Gary S. Miliefsky, CEO of SnoopWall ([www.snoopwall.com](http://www.snoopwall.com)) said ratters can:

- Download, upload and delete your files (potentially even clearing a hard drive completely)
- Steal passwords, credit card numbers, emails and files
- Watch you type and log your keystrokes
- Watch your webcam and save videos
- Listen in on your microphone and save audio files
- Take control of your computer
- Overclock your CPU to physically destroy it
- Install additional tools including viruses and worms
- Edit your Windows registry
- Use your computer for a distributed denial of service (DDoS) attack

RATs are effective delivery systems for the perpetrators behind botnet and phishing attacks, spreading SPAM, and storing illegal data. RATs have also been used to set up software that mines cybercurrency such as bitcoins.

“A ratter who gains access to your devices can quickly get control of your email address book, which in turn can be used to spread the malware to accounts belonging to friends and family”. As Miliefsky said: “If you get infected with one of these zero-day RATs, you’re not only a victim, you are an accidental accomplice.”<sup>5</sup>

All these functions can be activated with no warning.

## WHERE ARE THE VULNERABILITIES IN MY DEVICES?

Zero-day exploits leave even the most up-to-date computers open to malware. Once exploited, “Many RATs can disable antivirus and firewall software or create covert channels to bypass them.” Miliefsky says.<sup>6</sup>

Vulnerabilities aren’t limited to the operating system level. Many exist within specific applications. Although most operating systems and web browsers automatically download patches and security updates, many applications do not. And while manufacturers release these security

<sup>5</sup> [http://www.snoopwall.com/wp-content/uploads/2014/12/2015-Year-of-The-Rat-by-Gary-S-Miliefsky-SnoopWall\\_downloadPDF.pdf](http://www.snoopwall.com/wp-content/uploads/2014/12/2015-Year-of-The-Rat-by-Gary-S-Miliefsky-SnoopWall_downloadPDF.pdf)

<sup>6</sup>IBID



updates, it's often a manual process to download and install the patch. Some users delay or ignore prompts to install updates. Hackers exploit these gaps or holes in the code.

Failure to change the default password or settings on a device or application when installed to a network – even a home network – is another source of exposure to RAT infection. It's easy to find out the default ID and password for home routers. This ID/password combination is the first one hackers check when looking to infiltrate your system.

Many companies still run Windows 2003 Server even though Microsoft no longer supports it. As a result, any new vulnerabilities that are found are not patched. Companies knowingly expose themselves to this risk.

### HOW IS A RAT SPREAD?

The RAT is often “delivered” to your device by a phishing email or an infected download commonly disguised as a movie or song. In *Digital Peepholes*, a research paper examining the threat that hacked webcams pose to privacy, Kent College of Law Professors Lori Andrews, Michael Holloway, and Dan Massoglia reported that ratters disguise RATs as popular songs, then upload them to torrent sites.<sup>7</sup> Stolen music sites provide ratters with little resistance and easy prey: young people looking for free music, unaware of the danger the wrong file can bring.

In *Selling “Slaving,”* Digital Citizens researchers exposed conversations between ratters on the popular hackers' chat room Hack Forums. We saw many people advising less-experienced counterparts on the use of YouTube and content theft sites such as Pirate Bay and Kickass Torrents to spread their RATs.

This report contains research and interviews the Digital Citizens Alliance has compiled since 2015. Digital Citizens has found that RATs are frequently spread through content theft sites. Researchers from RiskIQ working on the report, Digital Bait, found that users are 28 times more likely to be infected with malware when visiting content theft sites. They found some of the most common sites include Xtreme RAT, Bifrost, and Back Orifice.

<sup>7</sup> <http://ckprivacy.org/publications/digital-peepholes/>



# DISSECTING A RAT

For nearly two decades, RATs have been a threat to Internet safety. As RATs become more sophisticated and more widespread, the threat increases. Also, more people are now online and this provides more opportunities for hackers to gain access to others' computers.

For readers who may not be familiar with some of the terms in this report, we offer the following definitions:

- **Script Kiddie** is a derogatory term used by more sophisticated crackers of computer security systems (aka hackers) to describe the less mature exploiters of security lapses on the Internet.<sup>8</sup>
  - Script Kiddies rely on RATs with a GUI to create the malware they want to use, and generally do not create the RAT on their own.
- **Application Programming Interface (API)** is a message format used by an application to communicate with the operating system or some other control program.<sup>9</sup> In short, APIs are what make it possible to move information between programs.<sup>10</sup>
  - For RATs, this allows the hacker to move data between the command and control server and the victims' systems. It also enables the hacker to make connections to the operating system to control the camera or microphone remotely.
- **Graphical User Interface (GUI)** allows users to interact with electronic devices through icons and visual indicators, as opposed to text-based interfaces, typed command lines, or text navigation.<sup>11</sup>
  - When a RAT has a GUI, it allows script kiddies to use RATs more easily.
- **Command and Control Servers (CnC or C&C)** are centralized machines that are able to send commands to, and receive outputs from, machines that are part of a botnet.<sup>12</sup>
  - If the RAT is used for a 1:1 attack, the hacker's system is also the CnC server.

We have included a few video examples of some of the best-known and most dangerous RATs. The balance of the report is sectioned by category. We have not included Category I applications, as these are legitimate tools. The first section covers RATs geared toward script kiddies. The second covers RATs employed by higher-level organizations, such as criminal groups. The last concerns RATs used by nation-states.

<sup>8</sup> <http://searchmidmarketsecurity.techtarget.com/definition/script-kiddy>

<sup>9</sup> <http://www.pcmag.com/encyclopedia/term/37856/api>

<sup>10</sup> <http://readwrite.com/2013/09/19/api-defined>

<sup>11</sup> [https://en.wikipedia.org/wiki/Graphical\\_user\\_interface](https://en.wikipedia.org/wiki/Graphical_user_interface)

<sup>12</sup> A botnet is a group of computers connected in a coordinated fashion for malicious purposes. Each computer in a botnet is called a bot. These bots form a network of compromised computers, which is controlled by a third party and used to transmit malware or spam, or to launch attacks. A botnet may also be known as a zombie army. (<http://www.techopedia.com/definition/384/botnet>)



# DIFFERENT BREEDS OF RATS

## SUBCATEGORIES OF RATs:

- **Category I: Legitimate applications**, produced by known vendors and used as described above, as Remote Access Tools (see next page for explanation on difference between tools and Trojans).

II

- **Category II: Applications written by others** that have the ease-of-use features that make them less complicated to distribute and to monitor the victims they infect. These RATs are **used by script kiddies or wannabe hackers** who do not have the skills to write their own RATs.

III

- **Category III: Applications written as criminal tools.** Criminal organizations are highly sophisticated and have the technical resources to write a higher level of application. Although these organizations also use Category II applications, they develop and employ a more robust set of RATs.

IV

- **Category IV: Applications written by nation-states.** These have the highest level of complexity and are usually closely guarded and the most difficult to detect. Nation-states use Category II and Category III application as well, but they typically do not write that type of RAT.



## TOOL V. TROJAN

Some people use the term “Remote Access Tool” when describing Remote Access Trojans. They shouldn’t. There’s a big difference between “Remote Access Trojans” and “Remote Access Tools.” A “Remote Access Tool” is used by IT professionals. It is a legal and helpful application. The “Tool” does some of the same things as the malware ratters call a Remote Access Trojan. Both applications have the same purpose: each allows a person to access and “control” another’s computer. But for a tool to work, the user must invite the operator to access the device. There is no invitation needed for the Trojan, designed to infiltrate the computer and bypass security. Once the user has unwittingly opened a “backdoor,” the Trojan enables another to take control without the user’s permission. You can turn off a tool at any time, but the Trojan is very difficult to eradicate.

Some people – including the moderators at the Hack Forums site - prefer using the word “Administration” instead of “Access”, but that does not change the meaning.

This report will only discuss the Trojans, not the tools. Therefore we will only be examining applications in Categories II-IV discussed above.



## CATEGORY II: COMMON RATS

As stated above, these RATs are typically used by the less skilled hackers known as script kiddies, who take advantage of built-in components such as GUIs and APIs to operate them. Most are also available for little or no money on the Internet.

### Back Orifice

**OVERVIEW:** Designed by The Cult of the Dead Cow in 1998, this RAT targeted Windows 98 systems and was later upgraded to Back Orifice 2000 to attack Windows 2000 and XP systems.

Back Orifice is one of the original RATs that included an API to make it easier for the hacker to access and remotely manipulate the Trojan once installed. The RAT also comes with a GUI, making it easier for script kiddies or non-technical people to deploy it.



**USAGE AND ADDITIONAL INFORMATION:** Back Orifice was found on airport systems in 2005, using its keylogger function to send keystrokes to a Hotmail account every 15 minutes.<sup>13</sup> Back Orifice was also used to gain access to a U.S. university, as well as an Australian mail server.<sup>14</sup> In the case of the university, the actual attack method was never determined, but it is assumed to be a music or video file downloaded with Back Orifice hidden inside. When the students shared the file around the university's network, presumably the RAT traveled with it.<sup>15</sup> In the report Digital Bait by RiskIQ and the Digital Citizens Alliance, published in December 2015, Back Orifice was ranked 3rd in the top 10 RATs found on content theft sites during the RiskIQ scans.

<sup>13</sup><http://www.securityfocus.com/news/11324>

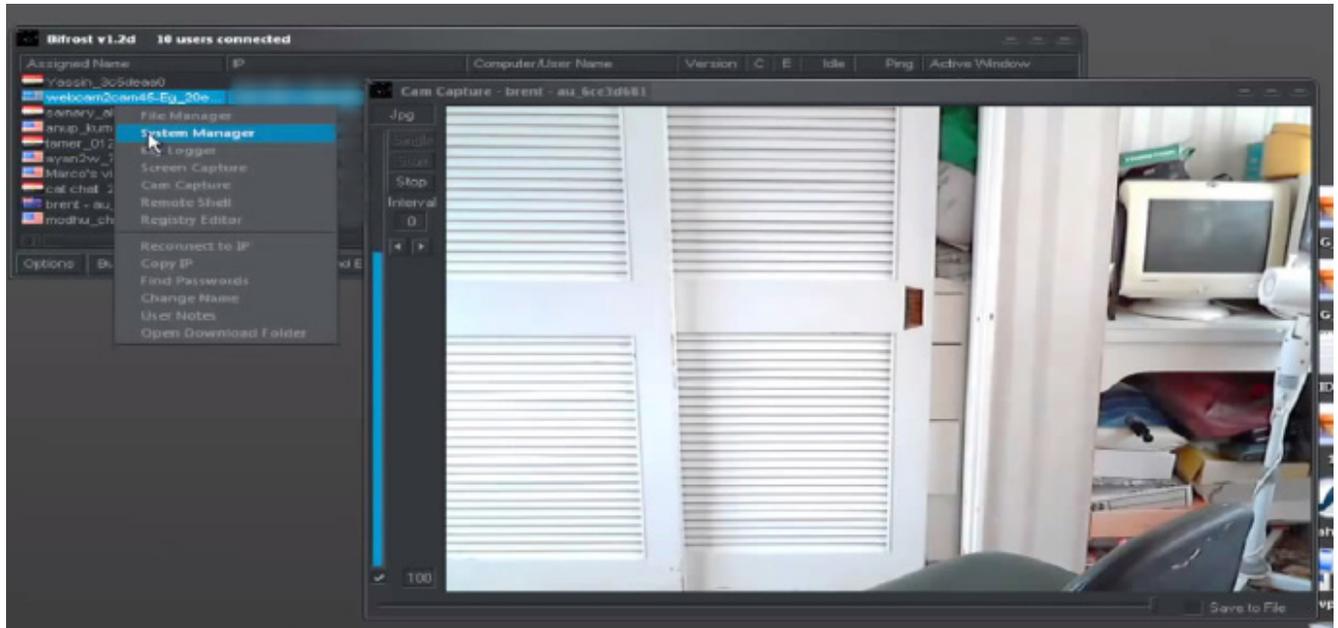
<sup>14</sup>[Pen-testing.sans.org/resources/papers/gcih/tracking-orifice-troajn-university-network-101743](http://Pen-testing.sans.org/resources/papers/gcih/tracking-orifice-troajn-university-network-101743)

<sup>15</sup>IBID



## Bifrost

**OVERVIEW:** Bifrost originated in Sweden in 2004.<sup>16</sup> Once installed on its victim's device, Bifrost has a GUI and powerful toolset. In *Selling "Slaving"*, re-researchers showed how hackers used Bifrost to exploit a young girl in Australia.



**USAGE AND ADDITIONAL INFORMATION:** As the above picture shows, the hacker has the ability to control the computer system, files, camera, and registry from this RAT.

In 2007, a North Carolina man, Ivory D. Dickerson, was sentenced to 110 years in jail for sending emails and instant messages to underage girls to get them to download the Bifrost Trojan. Once the Trojan was installed, Dickerson used the information he gained from the girls' systems to coerce his young victims to send him lurid photos.<sup>17</sup> FBI investigators found 600 images of child pornography on his computer.

Bifrost was ranked 2nd in the top 10 RATs found on content theft sites during the RiskIQ scans according to the report Digital Bait by RiskIQ and the Digital Citizens Alliance.

<sup>16</sup><http://www.threatexpert.com/files/Bifrost.exe.html>

<sup>17</sup>[http://www.nytimes.com/idg/IDG\\_002570DE00740E18002573A8007EA561.html?ref=technology](http://www.nytimes.com/idg/IDG_002570DE00740E18002573A8007EA561.html?ref=technology)



## Blackshades

**OVERVIEW:** Blackshades, published in 2010, was best known for its easy deployment. Security expert Brian Krebs wrote that Blackshades “was a tool created and marketed principally for buyers who wouldn’t know how to hack their way out of a paper bag.”<sup>18</sup>



**USAGE AND ADDITIONAL INFORMATION:** Cassidy Wolf, 2013 Miss Teen USA, has been a leading advocate for the concerns of RAT victims after her device was slaved and a ratter harassed her. She talked about her story with Digital Citizens Alliance researchers for their report, [Selling “Slaving.”](#) After she publicly shared her story, the FBI arrested 90 people – all allegedly sellers or users of Blackshades, but not before the malware infected more than 500,000 devices.<sup>19</sup> Before the arrests, Blackshades generated \$350,000 in sales between September 2010 and April 2014. Authorities found 6,000 customer accounts from more than 100 countries.<sup>20</sup>

Jared James Abrahams, a 19-year-old computer science student from Temecula, California, was sentenced to prison for taking control of Miss Wolf’s computer, taking pictures of her without her knowledge or permission, and then attempting to “sextort” her. While Miss Wolf was able to fend Abrahams off, he succeeded in slaving 150 devices and forcing some of his victims to make videos for him.

In the report, Digital Bait, Blackshades was ranked 7th in the top 10 RATs found on content theft sites during the RiskIQ scans cited in that report.

<sup>18</sup><http://krebsonsecurity.com/2014/05/blackshades-trojan-users-had-it-coming/>

<sup>19</sup>[http://www.nytimes.com/idg/IDG\\_002570DE00740E18002573A8007EA561.html?ref=technology](http://www.nytimes.com/idg/IDG_002570DE00740E18002573A8007EA561.html?ref=technology)

<sup>20</sup><http://www.news.com.au/world/breaking-news/blackshades-hackers-hit-aussies-kiwis/story-e6frfkui-1226923655784>



Authorities say he victimized other young women surreptitiously, by taking control of their computers and photographing them as they changed their clothes.<sup>21</sup>

Blackshades developer Alex Yucel was arrested in 2013. In 2015 he was sentenced to four years and nine months in prison and fined \$200,000.<sup>22</sup> Blackshades co-creator, Micheal Hogue, 23, of Maricopa, Arizona, pleaded guilty in January 2013 to two counts of computer hacking.

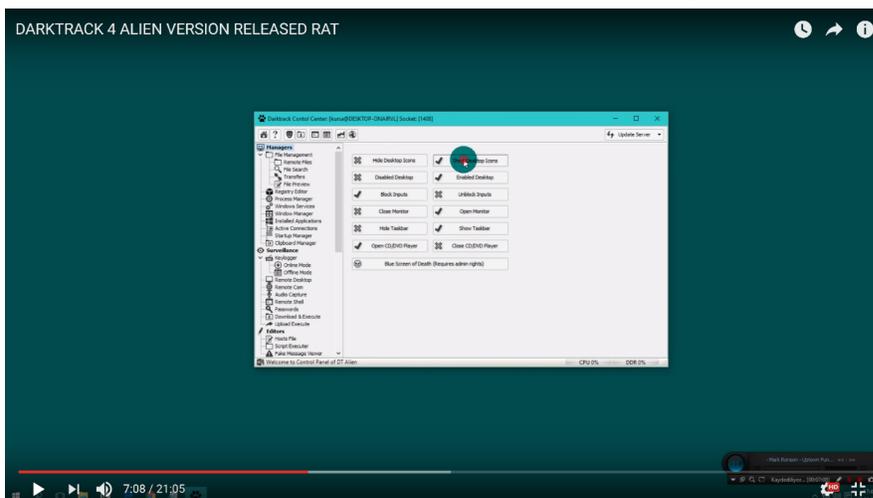
<sup>21</sup><http://www.cnn.com/2013/09/26/justice/miss-teen-usa-sex-tortion/>

<sup>22</sup>[http://www.wsj.com/article\\_email/blackshades-leader-sentenced-to-prison-1435093984-IMyQjAxMTA1MzlyMzMzOTM3Wj](http://www.wsj.com/article_email/blackshades-leader-sentenced-to-prison-1435093984-IMyQjAxMTA1MzlyMzMzOTM3Wj)



## DarkTrack

**OVERVIEW:** First seen in 2016, DarkTrack was created as a free remote access tool created by a developer by the name of Luckyduck. When discovered by MalwareHunterTeam, the RAT was considered as good as any RAT, free or paid, on the market. According to a Virus Guides article, “The Darktrack(sic) RAT is advertised to have some of the same strong features, common for commercial RATs like JBifrost (Adwind) or Orcus. Darktrack is able to spy via webcams, to connect to remote computers and access their filesystem, to dump passwords, to perform network stress tests (DDoD attacks), to log keystrokes, to execute commands on infected PCs, and interact with local processes and services.”<sup>23</sup>



**USAGE AND ADDITIONAL INFORMATION:** Unlike other RATs, DarkTrack has its own website and Facebook page.<sup>24</sup> The creator, Luckyduck, said the software will always be free and has created a new version DarkTrack Alien 5.<sup>25</sup>

Being free and effective product does not take away from its ability to infiltrate systems. In April of 2017, DarkTrack 5.0 was used in a spearphishing attack against the Ukraine military. The attack, in the form of a prescription with a Word document attachment, installs DarkTrack on the user's system NioGuard Security Lab reports. When the victim opens the Word document, the RAT is injected into the svchost.exe file. From here, DarkTrack connects back to its Command and Control (C&C) server. All of the IP addresses for these servers are located in Russia.<sup>26</sup>

<sup>23</sup><http://virusguides.com/commercial-rats-face-serious-competition-freely-offered-darktrack/>

<sup>24</sup><http://news.softpedia.com/news/free-darktrack-rat-has-the-potential-of-being-the-best-rat-on-the-market-508179.shtml>

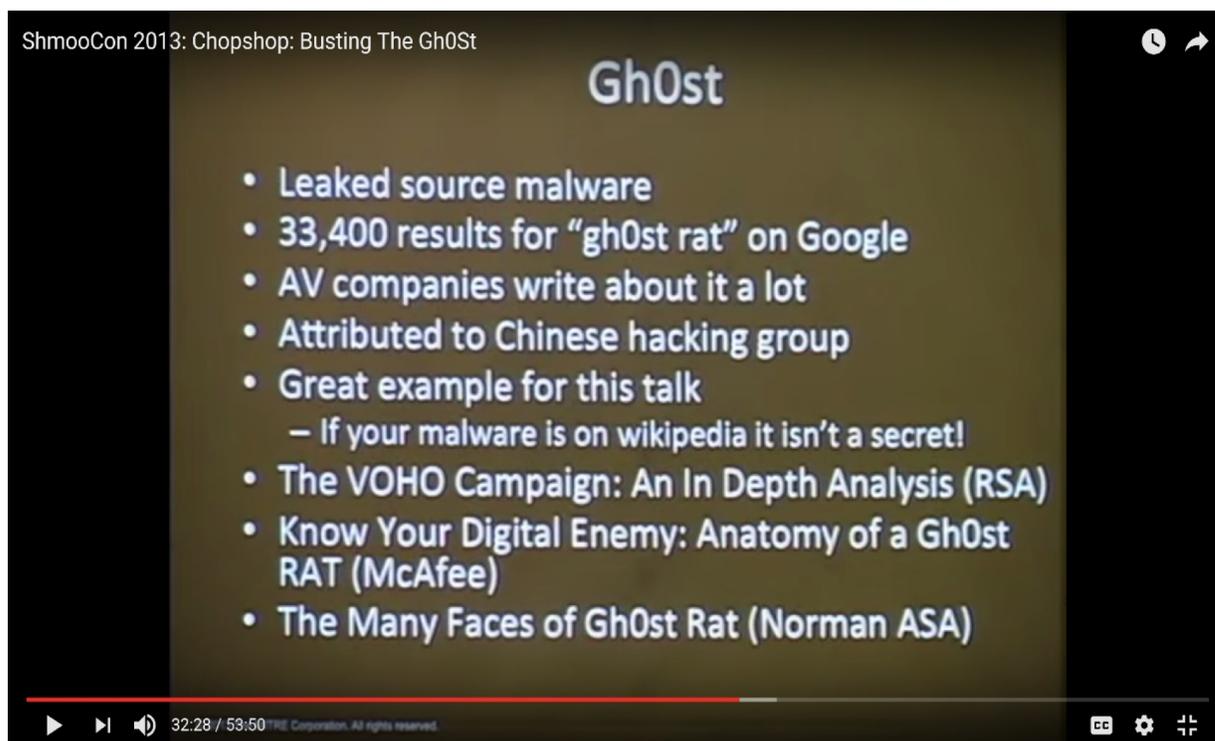
<sup>25</sup>ibid

<sup>26</sup><https://nioguard.blogspot.com/2017/05/targeted-attack-against-ukrainian.html>



## Gh0st Rat

**OVERVIEW:** Gh0st RAT has its roots back to the earliest Remote Access Trojans in the early 2000's. It has the same capabilities as other RATs in this paper, but Gh0st RAT was created and used as a nation-state tool developed in China.<sup>27</sup> Although Gh0st has been around a while, since its source code is available on the market, there are multiple variants of the RAT in the wild. According to a 2015 ThreatLabs article, there has been a six-year campaign of Advance Persistent Threats (APTs) using over 32 variants of Gh0st.<sup>28</sup>



ShmooCon 2013: Chopshop: Busting The Gh0st

### Gh0st

- Leaked source malware
- 33,400 results for "gh0st rat" on Google
- AV companies write about it a lot
- Attributed to Chinese hacking group
- Great example for this talk
  - If your malware is on wikipedia it isn't a secret!
- The VOHO Campaign: An In Depth Analysis (RSA)
- Know Your Digital Enemy: Anatomy of a Gh0st RAT (McAfee)
- The Many Faces of Gh0st Rat (Norman ASA)

32:28 / 53:50

**USAGE AND ADDITIONAL INFORMATION:** Gh0st's latest claim to fame is being used as one of the payloads in the WannaCry ransomware attack of 2017, but Gh0st has been used in other attacks as well.<sup>29</sup> According to FireEye, in July of 2017, two Chinese groups launched a "phishing campaigns against multiple companies in the aerospace and defense, construction and engineering, education, energy, health and biotechnology, high tech, non-profit, telecommunications, and transportation industries."<sup>30</sup>

<sup>27</sup><http://resources.infosecinstitute.com/gh0st-rat-complete-malware-analysis-part-1/#article>

<sup>28</sup><https://threatpost.com/eternalblue-exploit-spreading-gh0st-rat-nitol/126052/>

<sup>29</sup><https://threatpost.com/eternalblue-exploit-spreading-gh0st-rat-nitol/126052/>

<sup>30</sup>[https://www.fireeye.com/blog/threat-research/2015/07/demonstrating\\_hustle.html](https://www.fireeye.com/blog/threat-research/2015/07/demonstrating_hustle.html)

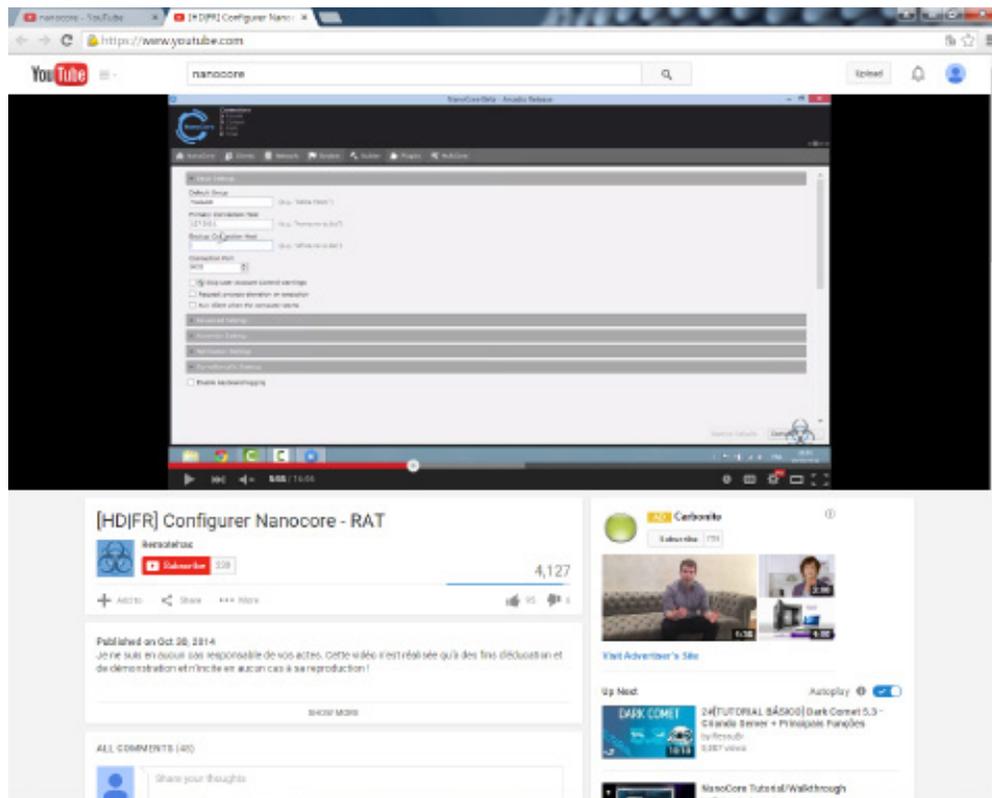


## NanoCore RAT

**OVERVIEW:** In 2013, the first version of NanoCore was released. In March 2015, a full version was released. In 2016, the original creator was arrested and the full source code leaked online.

Although creators of some versions of the RAT may charge a small price for the code, it is available at no cost as well. According to an online article posted by Net Security in March 2015, “what’s even worse for regular users, the cracked, full version of the RAT (with premium plugins) has been leaked online this month, and we can expect script kiddies to take advantage of the fact.”<sup>31</sup>

**USAGE AND ADDITIONAL INFORMATION:** According to a Symantec report, “One example we came across of NanoCore being used in a targeted attack involved a spam run that started on March 6. The targeted emails are being sent to energy companies in Asia and the Middle East and the cyber-criminals behind the attack are spoofing the email address of a legitimate oil company in South Korea.”<sup>32</sup>



(NOTE: The picture above not only has an advertisement with it, but the hacker uses the YouTube group to hide the real content of the RAT.)

<sup>31</sup>[http://www.net-security.org/malware\\_news.php?id=2995](http://www.net-security.org/malware_news.php?id=2995)

<sup>32</sup><http://www.symantec.com/connect/blogs/nanocore-another-rat-tries-make-it-out-gutter>



NanoCore incorporates a web freeware application, NirSoft, to do password retrieval. Although other RATs are using this tool, some researchers feel this RAT has a higher level of sophistication.<sup>33</sup> It also has several premium plugins such as a DDoS and keystroke logger. A report by security company enSilo further states: “NanoCore is undoubtedly one of the more sophisticated RATs out there. Given that NanoCore’s premium features are now freely available, we predict we’ll start seeing its usage in future cyber-attack campaigns.”<sup>34</sup>

<sup>33</sup> <https://www.ensilo.com/nanocore-rat-not-100-original/>

<sup>34</sup> IBID



**OVERVIEW:** njRAT was first detected in the wild in 2012. In June 2013, General Dynamics subsidiary Fidelis Cybersecurity reported an increase in attacks using the njRAT.<sup>35</sup> Beginning in 2015, njRAT has increasingly been used by the cyber arms of various Islamic terrorist groups such as ISIS and Al-Nusra. As recently as March of 2017 ISIS has used this program to spread malware to the computers of those who visit their sites.

**USAGE AND ADDITIONAL INFORMATION:** The attacks targeting government, telecom, and energy organizations were coming from “advanced threat actors in the Middle East, in particular when delivered via HTTP (i.e. Phishing attack or Drive-by download).”<sup>36</sup>



By April 2014, njRAT had spread around the world. Symantec reported 487 groups used njRAT for attacks, compromising “542 command and control (C&C) server domain names, and infecting 24,000 computers worldwide.”<sup>37</sup>

In the summer of 2014, Microsoft tried to disrupt the command and control of this family of RATs. Microsoft seized 23 domain names from provider No-IP. Microsoft states that this RAT was programmed to use these domain names for C&C. This led to “7.4 million infections of Windows PCs across the globe ... by malware developed in the Middle East and Africa.”<sup>38</sup> Despite Microsoft’s efforts, njRAT remains a prevalent RAT in the wild.<sup>39</sup>

In the report Digital Bait, published by Digital Citizens Alliance and RiskIQ, njRAT was ranked 4th in the top 10 RATs found on content theft sites during the RiskIQ scans.

<sup>35</sup> [http://www.fidelissecurity.com/sites/default/files/FTA\\_1009-njRAT\\_Uncovered\\_rev2.pdf](http://www.fidelissecurity.com/sites/default/files/FTA_1009-njRAT_Uncovered_rev2.pdf)

<sup>36</sup> IBID

<sup>37</sup> <http://www.v3.co.uk/v3-uk/news/2337382/middle-eastern-hackers-use-remote-access-trojan-to-infect-24-000-machines-worldwide>

<sup>38</sup> <http://thehackernews.com/2014/06/microsoft-seized-no-ip-domains-millions.html>

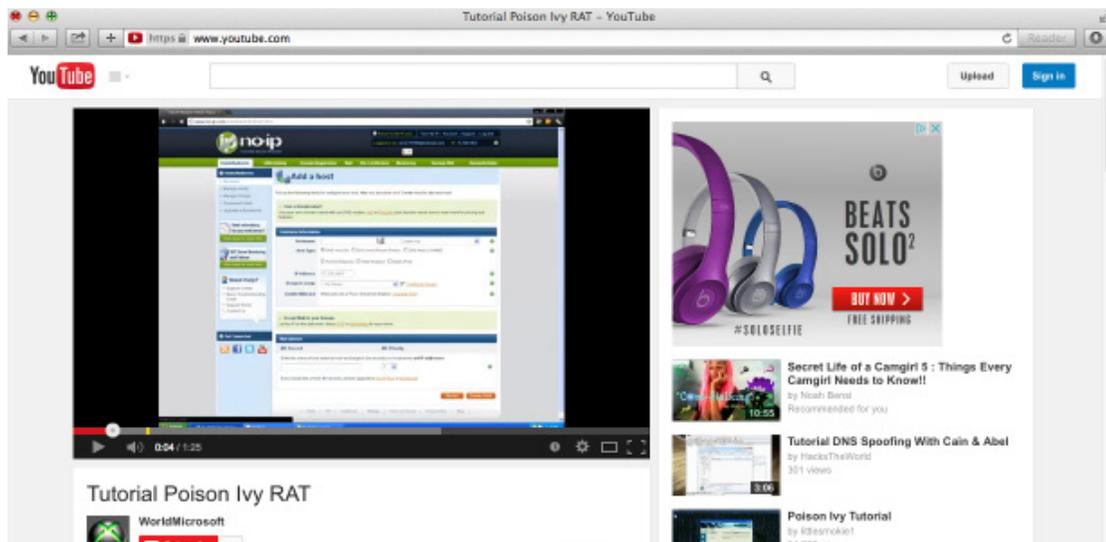
<sup>39</sup> <http://www.securityweek.com/njrat-infections-rise-security-firms>



## Poison Ivy

**OVERVIEW:** Poison Ivy emerged in 2006 and had its last variant around 2008.<sup>40</sup> Sources told Digital Citizens Alliance the creator of Poison Ivy is a woman living in the eastern USA. The Poison Ivy developer may go by the name Jonas.<sup>41</sup> In an August 2013 online article, FastCompany tells readers that the Poison Ivy website has support by a person named Codius who some think is the creator.<sup>42</sup>

According to a report by The Register, Poison Ivy RAT is the “AK-47 of cyber-attacks.” Poison Ivy is as ubiquitous a feature of cyber-espionage campaigns as the gun is to fighters all over the world.<sup>43</sup>



**USAGE AND ADDITIONAL INFORMATION:** The Register report also says it is the preferred RAT of Chinese cyber groups, but has been used in other parts of the world.

A campaign by a Middle Eastern hacking group called “MoleRATs” (aka Gaza Hackers Team) switched to Poison Ivy during June and July [2013] to attack Israeli government targets. “The latest malware was signed with a fake Microsoft certificate, similar to earlier attacks using the XtremeRAT trojan.”<sup>44</sup> Security Affairs website stated: “Security researchers subsequently linked these attacks to a broader, yearlong campaign that targeted not just Israelis but Palestinians as well — and, as discovered later, even the US and UK governments.”<sup>45</sup>

In December 2015, Digital Citizens Alliance and RiskIQ published the report Digital Bait, that ranked Poison Ivy 9th in the top 10 RATs found on content theft sites during the RiskIQ scans.

<sup>40</sup><http://dwatson.com/2013/04/14/a-rat-named-poison-ivy/>

<sup>41</sup>IBID

<sup>42</sup><http://www.fastcolabs.com/3015224/computings-11-smartest-super-viruses-and-the-damage-they-wrought>

<sup>43</sup>[http://www.theregister.co.uk/2013/08/27/poison\\_ivy\\_rat Apt/](http://www.theregister.co.uk/2013/08/27/poison_ivy_rat Apt/)

<sup>44</sup>[http://www.theregister.co.uk/2013/08/27/poison\\_ivy\\_rat Apt/](http://www.theregister.co.uk/2013/08/27/poison_ivy_rat Apt/)

<sup>45</sup><http://securityaffairs.co/wordpress/17229/cyber-crime/poison-ivy-still-alive-old-malware-new-cyber-threats.html>

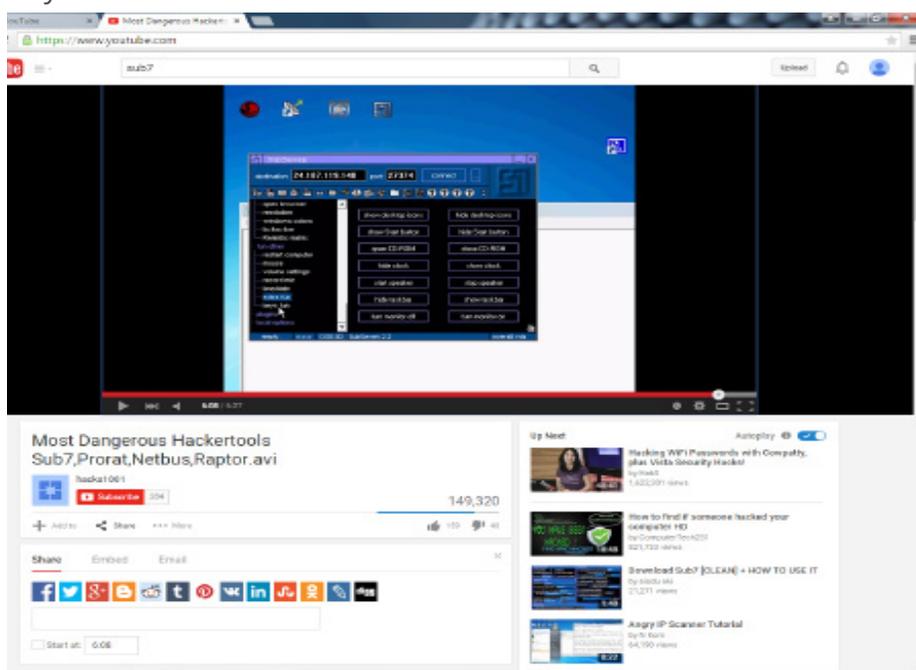


Poison Ivy is also used for 1:1 attacks. A “peeping Tom”-style webcam sextortionist, Luis Mijangos<sup>46</sup>, is now serving a six-year jail sentence in the US after targeting several young women in attacks that relied on a modified version of Poison Ivy.<sup>47</sup>

## Sub7

**OVERVIEW:** This Trojan was created in 1997 by Greg Hanis when he was a teenager. In a phone interview with Digital Citizens Alliance, Hanis says the original reason behind creating the RAT was to reduce the time needed by Hanis to strengthen a character in the game Ultima Online. He updated the RAT in 1999 by adding a GUI. It was discovered in 1999 and updates to the leading anti-virus signature tables were produced in early 2000. Sub7 was written in Delphi which makes it very hard to reverse engineer.

Like Back Orifice, Sub7 (or SubSeven or SubS3ven) was an early RAT with both GUI and API functions. The picture below shows some of the GUI menu options by which the hacker can manipulate the victim’s systems.



**USAGE AND ADDITIONAL INFORMATION:** Hanis discovered that he could employ the RAT to gain access to other people’s online IDs and passwords, allowing him to steal the victim’s virtual possessions. The Trojan is non-replicating and is usually spread through phishing attacks or chat rooms. Hanis further tells that he used chat rooms to distribute the RAT to other people playing the Massively Multiplayer Online Role-Playing Game (MMORPG) Ultima Online.

In the December 2015 report Digital Bait, published by Digital Citizens Alliance and RiskIQ, Sub7 was ranked 8th in the top 10 RATs found on content theft sites through the RiskIQ scans.

<sup>46</sup>[http://www.theregister.co.uk/2011/09/02/wheelchair\\_bound\\_webcam\\_pervert\\_jailed/](http://www.theregister.co.uk/2011/09/02/wheelchair_bound_webcam_pervert_jailed/)

<sup>47</sup><http://www.internet-security.ca/internet-security-news-archives-040/poison-ivy-rat-tool-used-in-complex-cyber-attacks.html>



Hanis would say he had “cheats” for the game and if other players wanted it, they should contact him. Hanis said, “I made an executable [the RAT], I sent it to them, they would double-click it and then I could NET USE over to their machine.” Once he had their credentials, he would log in to the game as the victim and trade all of their virtual possessions to his character. In another case, Sub7 was sent as a phishing attachment disguised as a fix to the Pinkworm viruses to Hotmail users in Japan.<sup>48</sup> (NOTE: There is no Pinkworm virus.) In another case, 800 systems were infected when the Trojan downloaded from a chat room site masqueraded as the movie SexxyMovie.mpeg.exe.<sup>49</sup>

According to Intel Security Group, “[t]he Trojan also registers the file extension .dl as an executable file type that can be run by the operating system just like any .exe file. This allows the attacker to download files onto the victims system and run them. Because the extension is not usually associated with executable files, some virus scanners will not scan these files and the victim will not suspect these files.”<sup>51</sup>

Hanis told Digital Citizens Alliance that the original version did not have a GUI. It was just a hard-coded program. Soon after the original version was created, Hanis had his friends using the RAT so they too could steal online possessions by sending the RAT to their friends. Most of Hanis’s friends did not understand how the program worked, so he created a GUI that made it easier for his friends to customize the RAT and send it out. While he was working on the GUI, Hanis researched what other RATs at the time were doing, like opening and closing CD-ROM drives. Hanis reached out to the developers of Back Orifice and others to discover other capabilities. He added a keylogger and screen sharing features to Sub7. Hanis said, “Then we just got to wait for the [victim] to log in and we got all this access.”

Another way Hanis distributed his RAT was through a process that he termed “melding.” He would get a program like Solitaire and “meld” or bundle-package Sub7 to it. When he sent the new file out, the victim would click on the file and the RAT would load, but then so would Solitaire. With this type of packaging, the victim did not know they were infected.

Like many teenagers, Hanis was more focused on the game than real life. He told Digital Citizens that he created the RAT only to be used with the online game. He never had any interest in using to spy on victims or steal actual information. When the RAT got out into the wild, he was upset that it was used for criminal purposes.

<sup>49</sup><http://www.giac.org/paper/gcih/189/investigation-subseven-trojan/103527>

<sup>50</sup><http://www.iss.net/threats/advise65.html>

<sup>51</sup><http://home.mcafee.com/virusinfo/virusprofile.aspx?key=10566>



## Xtreme Rat

**OVERVIEW:** This RAT was discovered in 2010. It was developed by a hacker known as xtremecoder. It is written in Delphi, the same development platform as SpyNet, CyberGate, Sub7, and Cerberus RATs.<sup>52</sup>

**USAGE AND ADDITIONAL INFORMATION:** Like Poison Ivy, XtremeRAT has been used to attack both companies and governments. It was used in 2012 for attacks on Israel and Palestine. It has also been used to attack high-tech companies, financial services companies, and energy/utility companies.<sup>53</sup> XtremeRAT was also used to attack some government agencies in the United Kingdom, Turkey, and the United States.



Unlike Blackshades, which charged \$40 for a copy of the application, XtremeRAT was available for free on the internet.<sup>54</sup>

In the report Digital Bait by RiskIQ and the Digital Citizens Alliance, XtremeRat was ranked 1st in the top 10 RATs found on content theft sites during the RiskIQ scans.

<sup>52</sup><https://www.fireeye.com/blog/threat-research/2014/02/xtremerat-nuisance-or-threat.html>

<sup>53</sup><https://www.fireeye.com/blog/threat-research/2014/02/xtremerat-nuisance-or-threat.html>

<sup>54</sup><http://securityaffairs.co/wordpress/25533/cyber-crime/fireeye-molerats-attacks-xtreme-rat.html>



## MOBILE RATs

As quickly as new defenses come into the market and awareness rises for computer-targeting RATs, new malicious applications are introduced. RSA Security reports that the next wave of RATs is being directed at smartphones, banking systems, control systems, and other targets.<sup>55</sup> Many of the current mobile RATs are similar to the other Category II RATs.

Smartphones get infected the same way computers do. The same phishing techniques work on these types of devices. However, smartphones are susceptible to text messages with embedded links and QR code on

advertisements whereby the user has no idea where their browser will be directed. According to a security expert we spoke to who wishes to remain anonymous, these attack vectors are just as effective as their computer counterparts, but the general public is not as aware of them.

Ratters also infect apps loaded on third-party app stores. Although you can still get malware from apps downloaded from Apple's App Store or Google Play, your odds increase if you download apps from third-party sites.

RSA Conference 2012 - Hacking Exposed: Mobile RAT Edition - Dmitri Alperovitch & George Kurtz

### Dawn of a New Era—Mobile RATs

- Mobile RATs
- Smartphones are PCs that fit in the palm of your hand
- Perfect tool to:
  - Intercept calls
  - Intercept TXTs
  - Intercept emails
  - Capture remote video
  - Listen to sensitive conversations
  - Track location via GPS



2:55 / 10:40

<sup>55</sup><https://www.rsaconference.com/blogs/mobile-security-vulnerabilities-are-creating-big-problems>



## Adwind-UNRECOM (Mobile)

**OVERVIEW:** Released between 2012 and 2013, Adwind, originally named Frutas, was created in Spain. It was later rebranded as UNRECOM (UNiversal REmote CONTROL Multi-platform).

This RAT has the ability to attack mobile and standard computer platforms from the same application. It is JAVA-based and JAVA is a very popular programming language. Adwind is sold for \$75 for a single copy and up to \$250 for multiple licenses.<sup>56</sup>

**USAGE AND ADDITIONAL INFORMATION:** Newer versions of the RAT are able to mine for Litecoins. “The inclusion of a Litecoin miner plugin is highly notable, given the slew of threats targeting cryptocurrencies we’ve seen recently. Litecoin is a cryptocurrency that’s often considered as a popular alternative to Bitcoin,” Trend Micro Threat Response Engineer Mark Joseph Manahan noted in a blog post.<sup>57</sup>



*The Litecoin-mining component is a plugin. It's worth noting that the creators of UNRECOM can add other plugins to further enhance the threat.*<sup>58</sup>

A version of this RAT has been written in Turkish and is spreading. According to Threat Geek, “we were detecting a Turkish-language Adwind hitting UK and US enterprises in the transportation and IT industries.”<sup>59</sup> This RAT allows the hacker to create packages for different types of operating systems (OS) on both computer and mobile platforms.

As you can see, Adwind can create a RAT targeting Microsoft, Android, Linux, and Mac. Having one tool that can attack multiple operating systems is a benefit to any hacker.

In the December 2015 report Digital Bait, published by Digital Citizens Alliance and RiskIQ, Adwind was ranked 5th in the top 10 RATs found on content theft sites during the RiskIQ scans sited in that report.

<sup>56</sup><https://techanarchy.net/2014/01/adwind-rat-analysis>

<sup>57</sup><http://news.softpedia.com/news/Java-RAT-UNRECOM-Mines-for-Litecoins-Infests-Android-Devices-438191.shtml>

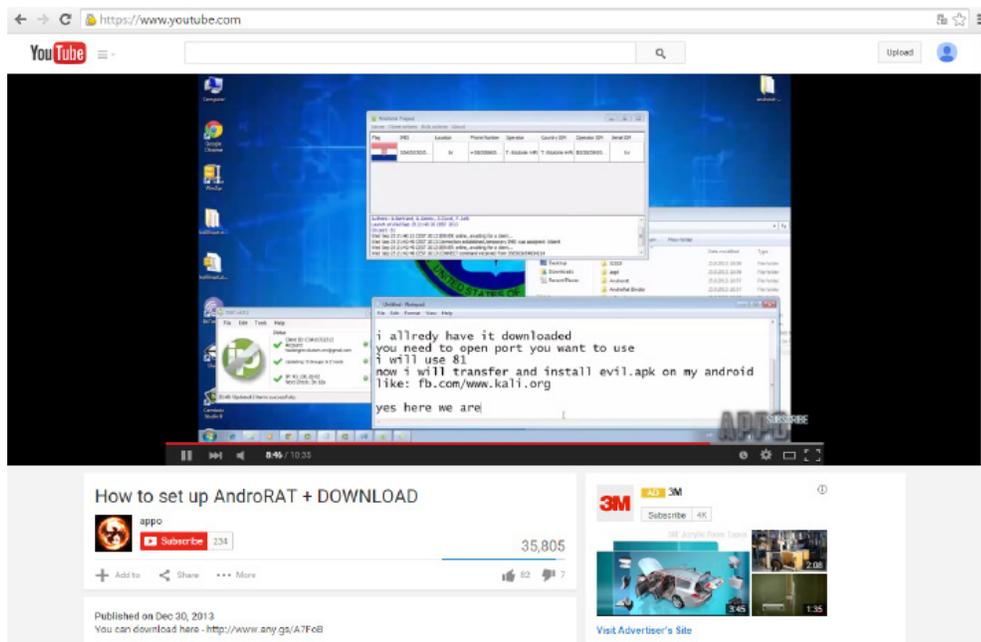
<sup>58</sup>IBID

<sup>59</sup><http://www.threatgeek.com/2015/04/adwind-continues-to-fly-now-using-turkish-language-lures.html>



## AndroRAT (Mobile)

**OVERVIEW:** Created as an open-source tool in 2013 by a team of French university students, this JAVA-based system is free.<sup>60</sup> There is a companion application, the AndroRAT APK Binder, that costs \$37 and allows a hacker “to Trojanize legitimate Android apps with a backdoor that lets miscreants access infected mobile devices remotely,” according to Symantec Researcher Andrea Lelli, in a *Krebs On Security* article.<sup>60</sup> In a PCMag article about AndroRAT, Lelli also said that the RAT “easily allows an attacker with limited expertise to automate the process of infecting any legitimate Android application with Androrat.”<sup>62</sup>



**USAGE AND ADDITIONAL INFORMATION:** Lelli also said, “For example, when running on a device, AndroRAT can monitor and make phone calls and SMS messages, get the device’s GPS coordinates, activate and use the camera and microphone, and access files stored on the device.”<sup>63</sup>

iOS has a much lower infection rate than other smartphone operating systems, but it still can get hacked.<sup>64</sup> It is recommended that both iPhones and Android devices have anti-malware installed on them. The mobile anti-malware software, like the anti-virus on your computer, will need to be kept up to date to minimize the risk of infection from RATs.

<sup>60</sup><http://securitywatch.pcmag.com/hacking/313775-android-remote-access-trojan-for-sale-cheap>

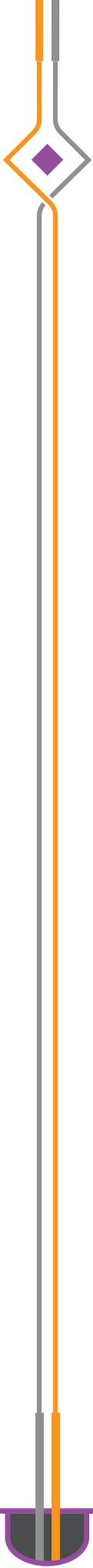
<sup>61</sup><http://krebsonsecurity.com/tag/andrea-lelli/>

<sup>62</sup><http://securitywatch.pcmag.com/hacking/313775-android-remote-access-trojan-for-sale-cheap>

<sup>63</sup><http://krebsonsecurity.com/tag/andrea-lelli/>

<sup>64</sup><https://www.sophos.com/en-us/security-news-trends/security-trends/malware-goes-mobile/why-ios-is-safer-than-android.aspx>





## UNCOMMON RATS

The RATs we reviewed in the sections below are used by sophisticated organizations such as criminal groups, disruptive political groups, or nation states. Although these groups also use RATs from the previous sections, the RATs discussed here are a bigger, meaner breed. Their enhanced capabilities include:

- Greater stealth than those we have already covered.
- Modular design allowing advanced users to write customized add-ons to the base system for specific targets.
- Less available source code not publicly shared, unlike that of the RATs in the above sections.



## CATEGORY III: CRIMINAL TOOLS

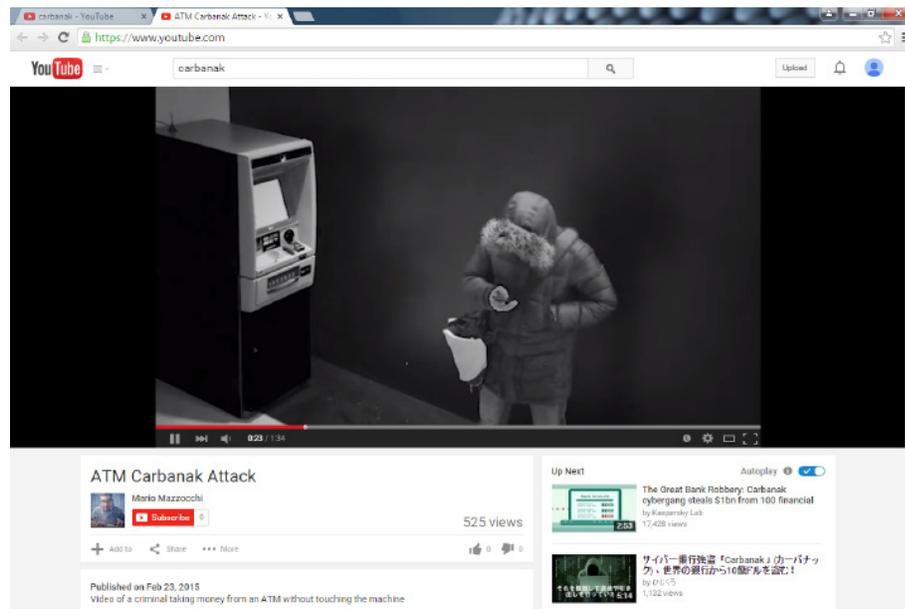
### Carbanak RAT (Banking)

**OVERVIEW:** An organization known as “Carbanak cybergang,” named for the RAT it used, may have transferred \$1 billion into its bank accounts. According to a story by InfoSec Institute, ratters used Carbanak to “hit more than 100 financial institutions in 30 countries ... the malicious campaign started in 2013 and there are strong indications that it may still be ongoing.”<sup>65</sup>

**USAGE AND ADDITIONAL INFORMATION:** This RAT attacks banks, not individuals. According to a New York Times article, “In late 2013, an A.T.M. in Kiev started dispensing cash at seemingly random times of day. No one had put in a card or touched a button. Cameras showed that the piles of money had been swept up by customers who appeared lucky to be there at the right moment.”<sup>66</sup>

“This is likely the most sophisticated attack the world has seen to date in terms of the tactics and methods that cybercriminals have used to remain covert,” said Chris Doggett, the former Managing Director of the Kaspersky North America office in Boston.<sup>67</sup>

But it was not only the ATM that had been hacked. Systems were also compromised inside the bank, where money transfers and bookkeeping are done, allowing the hacker to decipher the bank’s operations and to wire transfer funds to dummy accounts, thereby gaining access to the money.



<sup>65</sup><http://resources.infosecinstitute.com/carbanak-cybergang-swipes-1-billion-banks/>

<sup>66</sup>[http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html?\\_r=1](http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html?_r=1)

<sup>67</sup>IBID



A Computerworld UK report quoted Kaspersky Lab in describing the Carbanak attack. “We believe that the Carbanak campaign is a clear indicator of a new era in cybercrime in which criminals use APT techniques directly against the financial industry instead of through its customers. APTs are not only for stealing information anymore,” concludes Kaspersky Lab with some understatement.<sup>68</sup>

For all of its sophistication, the initial attack vector was a spear-phishing campaign. Once inside the bank, the Carbanak cybergang continued to use spear phishing to gain access to more systems with higher levels of administrative privileges.

<sup>68</sup><http://www.computerworlduk.com/it-vendors/1-billion-carbanak-bank-heist-how-it-was-done-3598101/>



## Dyreza/Dyre (Banking)

**OVERVIEW:** This RAT was found in the summer of 2014, attacking large financial institutions around the world. The Dyreza or Dyre Trojan is a man-in-the-middle RAT<sup>69</sup> designed to gather credentials of online transactions from its victims.

Luis Corrons-Granel, Technical Director of PandaLabs, said in a phone interview with Digital Citizens Alliance that banking Trojans like those similar to Dyre are some of the most sophisticated malware in place today. “Taking into account they are not only used to steal credentials from bank customers, but they usually have much more functionalities. They serve as remote access tools and they steal all kinds of information. ... They are quite advanced. ... Some of them really have good programmers. At the end of the day, they work as if it was a legal industry.”

**USAGE AND ADDITIONAL INFORMATION:** According to American Banker, Dyre is used “in combination with social engineering to defeat the two-factor authentication banks typically require for large wire transfers, researchers say. As a result, the attackers are siphoning large sums of money — \$500,000 to more than \$1 million at a time — into offshore accounts.”<sup>70</sup>

Part of the social engineering is a phishing campaign. “The emails associated with a campaign use the misspelled subject line ‘Unpaid invoic’ as well as the attachment ‘Invoice621785.pdf,’<sup>71</sup>” reports SecurityWeek.

Don Jackson of PhishLabs told SecurityWeek: “Historically, banking Trojans were used to steal account credentials of banking customers, but now, sensitive business data is being stolen from companies in the healthcare industry, retail, software industry and others.”<sup>72</sup>

Later in 2014, the same RAT was used to get victims’ credentials for their Salesforce.com accounts. An article in SC Magazine quoted Tom Weingarten, CEO of SentinelOne, as saying: “Dyre could be going after Salesforce credentials, possibly to enable theft of databases or to further spread the malware through a known source.”<sup>73</sup>

<sup>69</sup>A man-in-the-middle attack is one in which the attacker secretly intercepts and relays messages between two parties who think they are communicating directly with each other. (<http://searchsecurity.techtarget.com/definition/man-in-the-middle-attack>)

<sup>70</sup><http://www.americanbanker.com/news/bank-technology/sneaky-dyre-malware-bilks-corporate-bank-accounts-1073613-1.html>

<sup>71</sup><http://www.securityweek.com/us-cert-warns-dyre-malware-used-phishing-attacks>

<sup>72</sup>IBID

<sup>73</sup><http://www.scmagazine.com/salesforce-warns-of-dyre-malware-possibly-targeting-users/article/370366/>



# HOW DYRE WORKS

1. Attacker sends phishing email with link to zip file hosted on Dropbox, Cubby, etc.



2. User clicks link, downloading zip file, unzips file, and Dyre installs on computer



3. Dyre phones home to command and control



4. Dyre monitors all browser activity and activates when user visits banks and cloud apps



5. User visits target site and Dyre hooks into the browser and hijacks the SSL protection



6. Data sent to target site through a man-in-the-middle Dyre server in the clear



Source: Skyhigh Networks

74

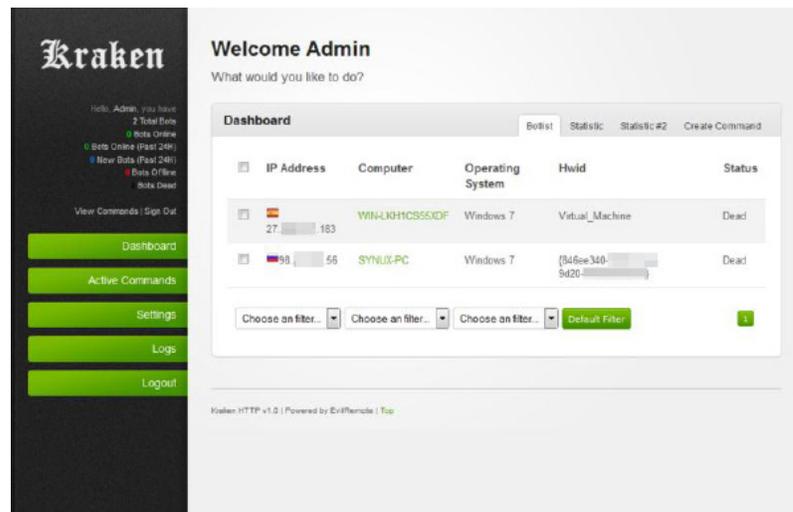
<sup>74</sup><https://www.skyhighnetworks.com/cloud-security-blog/dyre-straits-millions-of-cloud-users-vulnerable-to-new-trojan/>



## Kraken RAT (Bitcoin)

**OVERVIEW:** Originally released in 2008, Kraken was one of the largest botnets of its time. By 2009, the RAT was known and preventions were put in place. Developers updated Kraken in 2015 in order to target bitcoins.

Kraken is spread using spam attacks to which Microsoft Office documents are attached. These have been modified to exploit an old vulnerability. Users seem to be more likely to open the document than a URL.<sup>75</sup>



**USAGE AND ADDITIONAL INFORMATION:** Kraken “was said to be used during an espionage campaign against the energy sector, especially against targets in the UAE,” a G DATA SecurityBlog states. The article further says that Kraken is relatively unsophisticated. This may be by design or it may be that the hackers know they can exploit old vulnerabilities, since many companies do not patch older software.<sup>77</sup>

According to a Quick Heal report, “Exploit kits for targeting Bitcoins are readily available in the underground community and these are proving to be highly lucrative as well.” It further states that “Kraken RAT... is now being used for stealing Bitcoins and mining on infected systems.”<sup>78</sup>

According to the G DATA SecurityBlog article on Kraken, “[t]he Bitcoin monitor plugin is even more amusing. ... The malware monitors the infected user’s clipboard. If the user copies a Bitcoin address to the clipboard, it will be replaced by an address pre-configured by the botmaster.”<sup>79</sup>

<sup>75</sup><http://blogs.quickheal.com/wp/malware-case-study-kraken-rat-running-behind-bitcoins/>

<sup>76</sup><https://blog.gdatasoftware.com/blog/article/dissecting-the-kraken.html>

<sup>77</sup>IBID

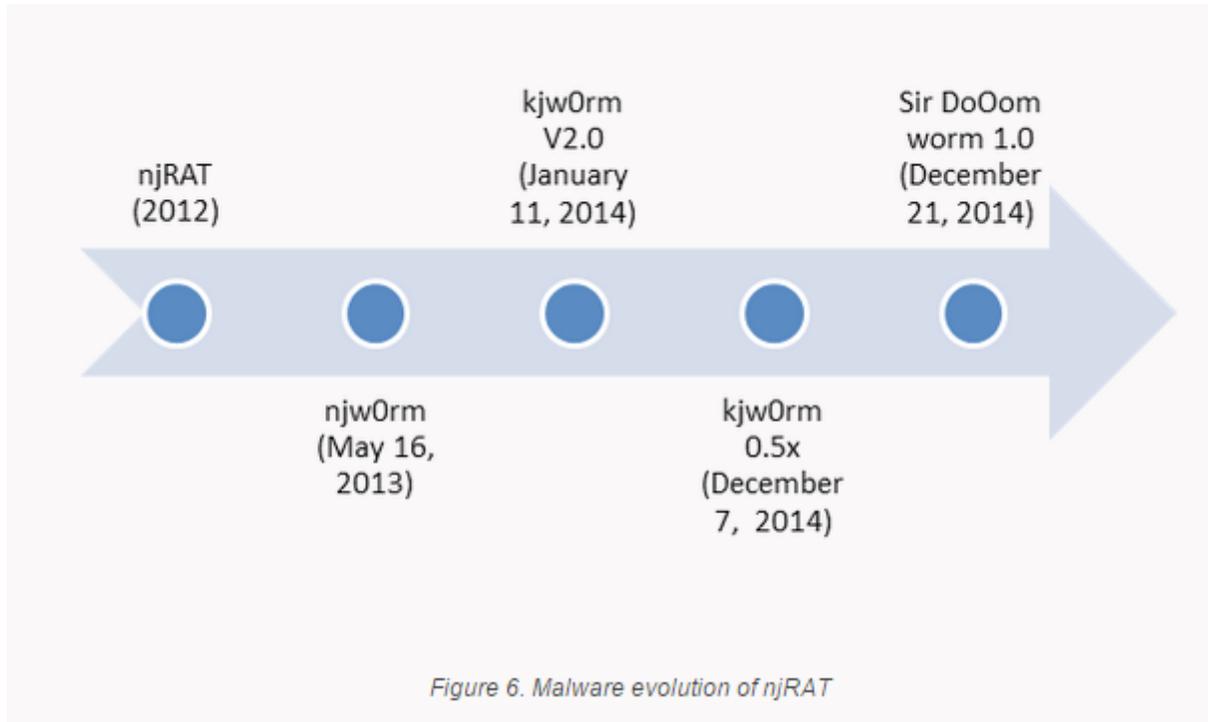
<sup>78</sup><http://blogs.quickheal.com/wp/malware-case-study-kraken-rat-running-behind-bitcoins/>

<sup>79</sup><https://blog.gdatasoftware.com/blog/article/dissecting-the-kraken.html>



## Sir DoOom

**OVERVIEW:** Sir DoOom (or Sir Do0om) is a modification of the njRAT (and the njw0rm), and was first released in December 2014. It has similar characteristics and capabilities as njRAT and is coded in Visual Basic Script.<sup>80</sup> Visual Basic Script is a very common language, like JAVA, which makes the RAT easier for a larger set of ratters to customize.



81

**USAGE AND ADDITIONAL INFORMATION:** Sir DoOom RAT has greater capabilities than those of njRAT. According to SecurityWeek, “Sir Do0om is even more interesting [than njRAT or njw0rm] since it can be used to mine Bitcoin, launch DDoS attacks, control computers based on a timer, display messages, terminate antivirus processes, and open a website related to [the] Quran, the central religious text of Islam. This RAT is also designed to terminate itself if the presence of a virtual machine is detected.”<sup>82</sup>

The Sir DoOom RAT has no released signature at the time of this research. Continue to update your anti-virus application so it will get the new definition once it is released.

<sup>80</sup><http://blog.trendmicro.com/trendlabs-security-intelligence/new-rats-emerge-from-leaked-njw0rm-source-code/>

<sup>81</sup><http://www.securityweek.com/njw0rm-source-code-used-create-new-rats>

<sup>82</sup>IBID



## CATEGORY IV: NATION STATE TOOLS

The RATs in this section are some of the most sophisticated pieces of malware yet found. Not only do they have a modular format and advanced stealth capabilities, their code is so advanced that some of it is not fully understood at this time.

### Explosive

**OVERVIEW:** This RAT seems to have evolved in Lebanon and was first used in 2012. There are five known variants.

The group called Volatile Cedar could have ties to the Lebanese government or another political group inside the country. The group is using this RAT to target defense contractors, telecommunications and IT companies, and media outlets as well as educational institutions. The group targets public-facing websites instead of the more typical attack vector of phishing, *Infosecurity Magazine* reports.<sup>83</sup> Once the website is infected, the RAT transfers itself from the web server into the internal servers on the network, where it steals data, deletes files, or performs arbitrary code executions.

**USAGE AND ADDITIONAL INFORMATION:** The RAT was used against Israeli and Turkish targets, employing several different methods to extract data, “including a keylogger, clipboard logger, memory monitor, and a means to check in with its command and control server.”<sup>84</sup> It also uses encrypted data links to transfer data. By using the different variants, the RAT is harder to track and can avoid anti-virus scanning.

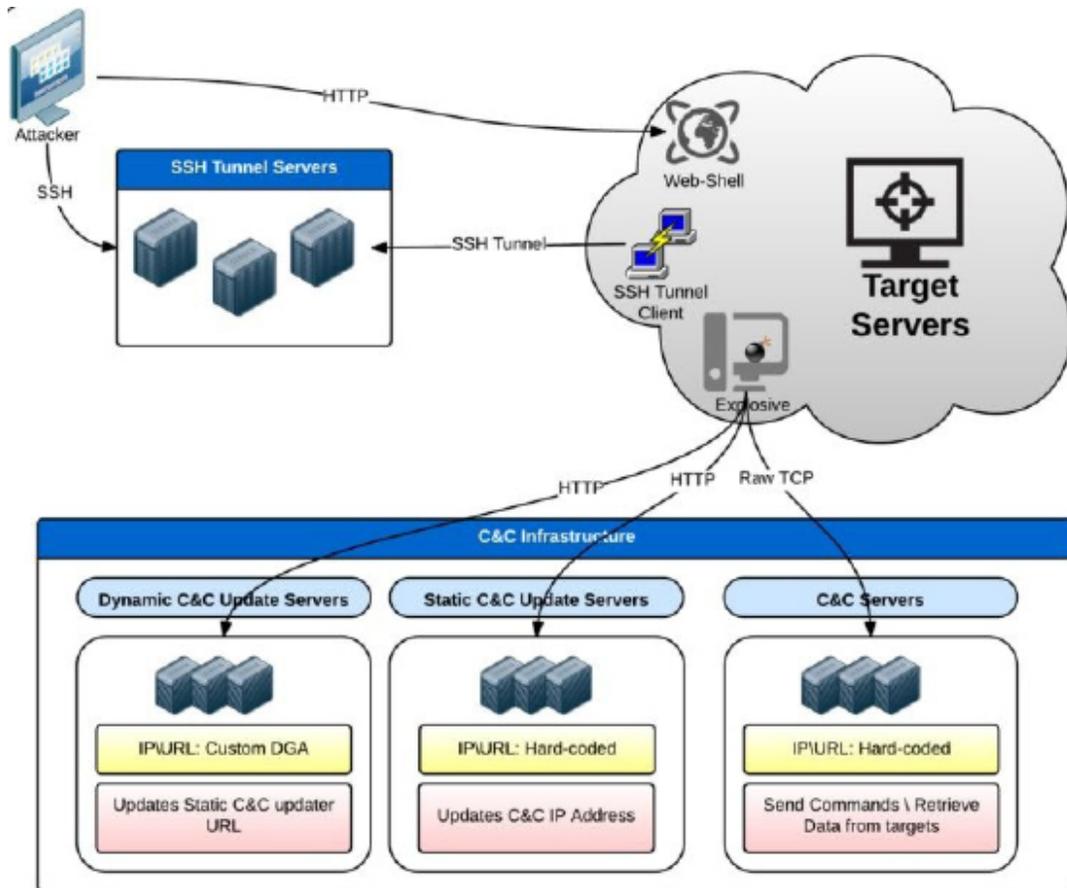
According to a document published by Check Point Software Technologies, the security firm and firewall manufacturer, “[t]he server framework is diverse. While some servers are owned (and possibly also hosted) by the attackers, other servers use publicly shared hosting frameworks or even compromised legitimate servers.”<sup>85</sup>

<sup>83</sup><http://infosecurity-magazine.com/news/explosive-apt-campaign-launched/>

<sup>84</sup><https://threatpost.com/volatile-cedar-apt-group-first-operating-out-of-lebanon/111895>

<sup>85</sup><https://www.checkpoint.com/downloads/volatile-cedar-technical-report.pdf>





86,87

A web report by Softpedia says the group Volatile Cedar “customized the Trojan for each target” and minimized network traffic during normal hours to avoid detection.<sup>88</sup> According to Dan Wiley, head of incident response and threat intelligence at Check Point Software Technologies, “This is one face of the future of targeted attacks: malware that quietly watches a network, stealing data, and can quickly change if detected by anti-virus systems.”<sup>89</sup>

<sup>86</sup><https://www.checkpoint.com/downloads/volatile-cedar-technical-report.pdf>

<sup>87</sup>C&C – Command and Control server. Same meaning as CnC previously defined in this document.

<sup>88</sup>[News.softpedia.com/news/Explosive-Malware-Used-by-Cyber-Espionage-Group-Working-from-Lebanon-477220.shtml](https://www.softpedia.com/news/Explosive-Malware-Used-by-Cyber-Espionage-Group-Working-from-Lebanon-477220.shtml)

<sup>89</sup>[http://www.theregister.co.uk/2015/04/01/lebanon\\_explosive\\_cyberspy\\_mystery\\_campaign/](http://www.theregister.co.uk/2015/04/01/lebanon_explosive_cyberspy_mystery_campaign/)

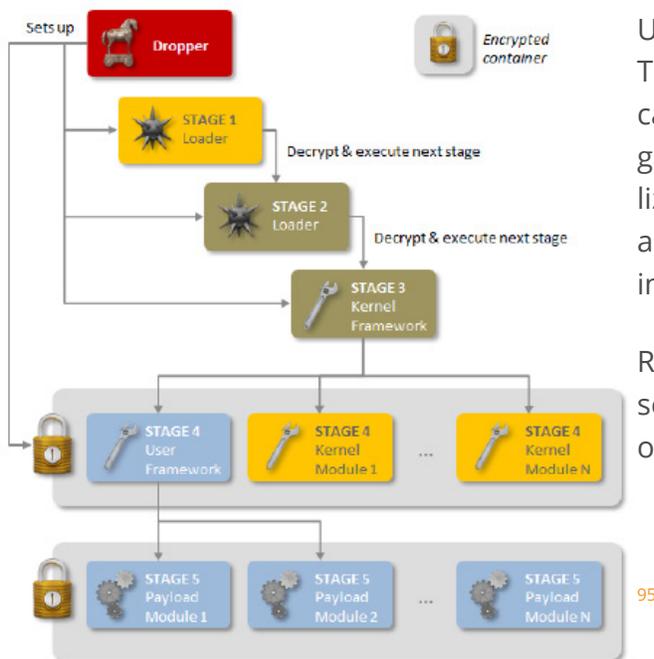


## Regin (Industry)

**OVERVIEW:** According to US-CERT<sup>90</sup>, Regin was first found in late 2014 but had been avoiding detection since 2008.

When reporting about research from Kaspersky on Regin in 2015, The Register, described Regin “as the devil spawn of Stuxnet and Duqu.”<sup>91</sup> The Kaspersky researchers determined that Regin has many of the same elements as the QWERTY keylogger, which some publications say ties it to the National Security Agency (NSA), based on their understanding of documents made public by Edward Snowden.<sup>92</sup>

**USAGE AND ADDITIONAL INFORMATION:** According to Symantec, Regin has been used in spying campaigns since 2008. A newer variant came into the spotlight in 2013. Symantec also says, “Targets include private companies, government entities, and research institutes. Almost half of all infections targeted private individuals and small businesses. Attacks on telecoms companies appear to be designed to gain access to calls being routed through their infrastructure.”<sup>93</sup>



US-CERT further states, “Regin is a remote access Trojan (RAT), able to take control of input devices, capture credentials, monitor network traffic, and gather information on processes and memory utilization. The complex design provides flexibility to actors, as they can load custom features tailored to individual targets.”<sup>94</sup>

Regin displays a level of complexity never before seen in a RAT, and is well-suited for long-term espionage against its targets.

<sup>90</sup>United States Computer Emergency Readiness Team

<sup>91</sup>[http://www.theregister.co.uk/2015/01/28/malware\\_bods\\_find\\_regin\\_malware\\_reeks\\_of\\_warriorpride/](http://www.theregister.co.uk/2015/01/28/malware_bods_find_regin_malware_reeks_of_warriorpride/)

<sup>92</sup>IBID and <http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html>

<sup>93</sup><http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance>

<sup>95</sup><https://www.us-cert.gov/ncas/alerts/TA14-329A>

<sup>95</sup><http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance>



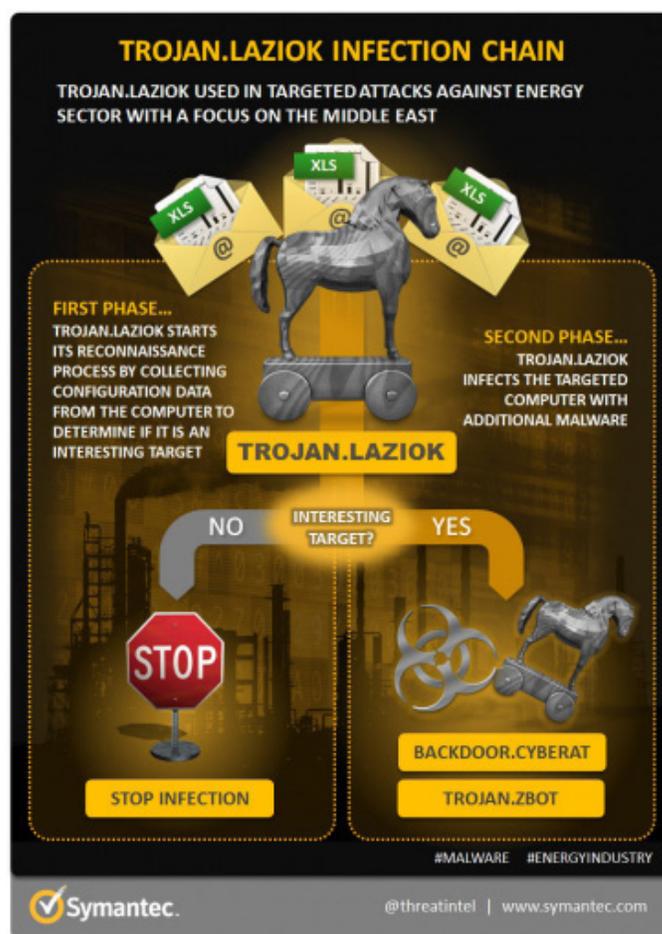
## Trojan.Laziok (Energy)

**OVERVIEW:** This RAT was discovered in early 2015. Like many attacks, this starts as a spam or phishing campaign. Once the tool is in place, it gathers information and sends it to the attacker. Once the attacker has the data, they determine which systems are the best targets to attack. The attacker then loads other malware such as Trojan.Zbot or Backdoor.Cyberat. These steal data and other information while leaving backdoors open, so the systems are vulnerable to further exploit.

**USAGE AND ADDITIONAL INFORMATION:** An April 2015 article on Security Affairs website quoted Symantec's blog: "[b]etween January and February, we observed a multi-staged, targeted attack campaign against energy companies around the world, with a focus on the Middle East. This attack campaign used a new information stealer detected by Symantec as Trojan.Laziok. Laziok acts as a reconnaissance tool allowing the attackers to gather data about the compromised computers."<sup>96</sup> According to Fortune.com, "Because most of the companies singled out are involved in the energy business, Symantec speculated that the hackers are motivated by industrial espionage."<sup>97</sup>

Industry experts agree that the attackers have not adopted advanced hacking techniques. They exploit old vulnerabilities using tools readily available in the hacking community.

This illustrates another reason why keeping your systems patched is critical to data security.



98

<sup>96</sup><http://securityaffairs.co/wordpress/35567/cyber-crime/energy-companies-laziok-trojan.html>

<sup>97</sup><http://fortune.com/2015/03/31/spies-malware-energy-email/>

<sup>98</sup><http://www.symantec.com/connect/blogs/new-reconnaissance-threat-trojanlaziok-targets-energy-sector>



# POPULAR PLACES FOR RATs

There are many places to find RATs and to learn how to use them. Some are buried on the Dark-Net, but ratters do discuss places to find and learn about RATs on the clear web as well. When we looked at sites such as Hack Forums, many individuals posted that the best ways to deploy their RATs were via YouTube or Reddit.

The screenshot shows a forum thread on Hack Forums. The thread title is "4 Unique ways to Spread on Reddit and Youtube" and it was posted by user "waqob" on 03-29-2015 at 10:43 AM. The thread contains several posts with detailed instructions on how to spread RATs using YouTube and Reddit. The first post by "waqob" provides a list of sites and methods, including using YouTube to spread malware by advertising fake video game cheats. The second post by "heisenberg410" provides more specific instructions on how to use Reddit to spread RATs, including using social engineering to convince users to download the program. The thread also includes a signature for "waqob" and a signature for "heisenberg410".

Thread Rating: [Progress Bar] New Reply

Thread Options

Post: #1

**waqob**  
[bin@HF:]  
Prestige: 8  
Posts: 269  
Joined: Nov 2014  
Reputation: 4

I'm going to share with you spreading methods that I use and worked for me.

Before you start here's a list of sites that do and don't distribute:  
<http://www.hackforums.net/showthread.php?tid=3557962>

**1. Youtube**

Yes, yes the old **Youtube** method I'm sure you've already used this. You advertise a fake video game cheat then watch desperate noobs download it. Unless you have bots/multiple accs that like and comment on your video to make it seem more legit, many people will already expect malware from your video and many will probably avoid it.

Instead, try a more different approach that people wouldn't expect that they'll get infected.

1a. First, download a remix of a song that's popular right now (It has to be a remix because there are probably thousands of **Youtube** videos of said song. And if you know how to make music then use this to your advantage) . Bind the .mp3 file with your RAT. Now upload the remixed song onto **Youtube** with the download link to your RAT. Thousands of unsuspecting users will download it.

1b. Go on a **Youtube** video with lots of views and comments covering a major news topic like Ferguson or Kim Kardashian. Post a comment containing a download link to your RAT claiming to be information on the topic.

**Reddit**

Because of how Reddit's system works it's going to be a bit more difficult than to pull this off. With **Reddit**, you will need to do a little social engineering to convince people to download your program. But if you do this right, you will get lots and lots of slaves. First of all, do not claim that you made the program. That will make other Redditors suspicious of you. Claim it's someone else's and you found it off a site. In fact, but you don't have to, link them to a fake webpage you made so they can really be convinced that it's not your program.

1a. On a topic, post a relevant comment with your download link or website and say "Oh yeah! I found this software/program, etc"

1b. Post a new topic. Make sure your binded program is relevant to the subreddit you are posting in. For example, on r/atheism make a RAT binded to an atheist wallpaper image and claim that you made a wallpaper for them to enjoy. (People don't expect for images to be viruses, you don't have to claim it was someone else's)

My signature

PM Find Quote Report

03-29-2015, 10:46 AM Post: #2

**heisenberg410**  
L33t Member  
Prestige: 35  
Posts: 1,057  
Joined: Jun 2014  
Reputation: 52



www.hackforums.net/showthread.php?tid=4802340

Current time: 05-06-2015, 02:04 PM

# Hack Forums

Packets, Punks, and Posts

Home Upgrade Search Members Extras Wiki Help Follow Contact

Welcome back, **outhaul4dca**. You last visited: Today, 12:07 PM (User CP — Log Out)  
 View New Posts | Your Threads | Your Posts | Private Messages (Unread 1, Total 1) Open Buddy List

Hack Forums / Hacks, Exploits, and Various Discussions / Hacking Tools and Programs / Remote Administration Tools / Searching for a good method to spread RATs

McDispenser  
Minecraft account generator

Buy Now

AffiliateFix

WIN \$500!

POST NOW

Thread Rating:  New Reply

**Searching for a good method to spread RATs** Thread Options

05-01-2015, 11:17 AM Post: #1

**Pider2k3**

[nobody@HF:]

Hi Boys,

i would love to hear about some methods how u spread your RATs.

I was using following methods till now:

- Sharing Cracked Software via Torrent
- Mass Chat Rooms
- Make Youtube Videos of Something and add your file.

can someone tell me some other methods how u spread your rats? Would love to try some new methods, cause im bored of always the same...

Thank you.

Prestige: 0

Posts: 11

Joined: Dec 2014

Reputation: 0

PM
Find

Quote
Report

« Next Oldest | Next Newest »


Search Thread
New Reply

Our researchers were able to find videos of the RATs in action. Many times, these videos include pictures of the victims using their devices with no idea they are being watched or that their system is being used to commit other cybercrimes.



# OBSERVING RATs - THE REMOTE ACCESS TROJANS OF THE PAST, PRESENT, AND FUTURE

In searches run in July 2017, Digital Citizens researchers scanned Hack Forums, Reddit, and YouTube for RATs that were generating discussion. Here are some of the newer names we found during our searches:

## List of RATs to watch

### Common

|                  |                  |               |
|------------------|------------------|---------------|
| Imminent Monitor | LuminosityLink   | Orcus         |
| Remcos           | Quasar           | Cardinal      |
| Bozok            | Astroid          | TheFatRAT     |
| SilentBytes      | Sakula           | KjW0rm        |
| Havex            | Agent.BTZ/ComRat | Dark Comet    |
| AlienSpy         | AlienSpy         | Chrome remote |
| JSpy             | Cyber Gate       | Pandora Rat   |
| DameWare RAT     | Pussy RAT        | jRAT          |

### Mobile

|            |           |       |
|------------|-----------|-------|
| RCSAndroid | DroidJack | Xsser |
| SpyNote    | Pupy      |       |

| Most Common RATs 2017 | Most Common RATs 2016 |
|-----------------------|-----------------------|
| DarkComet             | Dark Comet            |
| Chrome Remote         | Black Shades          |
| NjRat                 | JSpy                  |
| Jspy                  | Pussy RAT             |
| Black Shades          | Bozok RAT             |
| AndroRAT              | Poison Ivy RAT        |
| Pussy RAT             | NjRat                 |
| CyberGate             | DameWare RAT          |
| Pandora Rat           | jRAT                  |
| DameWare Rat          | Cyber Gate            |

99 100

DCA Researchers found one publication, CompsMag that ranked the most common RATs in the last two years (we have not seen or heard of CompsMag before and have not independently verified these results)

In 2005 DarkReading published *The 7 'Most Common' RATs In Use Today*, the list included: Sakula, KjW0rm, Havex, Agent.BTZ/ComRat, Dark Comet, AlienSpy, and Heseber BOT

<sup>99</sup> <https://www.compsmag.com/best-rat-2017/>

<sup>100</sup> <https://www.compsmag.com/top-best-rat-remote-administration-tool-tool-2016-security/>



## SUMMARY

Although new security standards keep coming out, it is not enough, says Greg Hanis. Many standards, like ISO or PCI, are not as focused as they could be. Hanis told DCA that when he does a penetration test,<sup>101</sup> he asks if the company wants the penetration test to focus on the needs of an audit, or if they want a level of penetration that better represents threats seen at the street level. “Think of it like a regulated boxing match with a referee and the other is like a street fight in a prison yard where they will [stab] and kill you.” Hanis feels that many standards are using the techniques they use in warfare for the kinetic world (i.e. conventional or limited warfare) and not digital world where anything is possible. “We need to be focusing more on detection,” says Hanis.

Dave Waterson, the CEO of SentryBay, made a similar comment in his blog. “Compliance often takes higher priority than real security. Clinging to outdated security solutions is rewarded and trying new ideas is risky,”<sup>102</sup> Waterson states in his blog.

As technology becomes more sophisticated, so do the strategies of the hackers. One grey hat hacker<sup>103</sup> who did not want their name disclosed told us criminals often keep each bot campaign to around \$3.5 to \$3.8 million. Why? Bot operators know that the FBI is understaffed and looking for headline

worth arrests an analyst said. The grey hat hacker continued, “they tend to pursue more higher-profile cases, meaning they will work a cases that in-volves ‘events’ that are upwards of \$4 million. The criminals are well-aware of this.”

Now consider that 1:1 attacks with RATs rarely generate that kind of reward. And there’s good reason for law enforcement to chase those creating banking Trojans. Luis Corrons-Granel, Technical Director of PandaLabs, told us that banking Trojans are some of the scariest malware he has seen.

Hanis, who now designs intrusion detection appliances for his company, Global Network Protection, is dismayed by lack of appropriate response and lack of centralized coordination. “There is no one to call,” says Hanis. If someone sees an issue and wanted to report it, who do you call? We are constantly told, “If you see something, say something.” But that mantra does not seem to apply to these types of crimes.

The lack of restraint seen by hackers and the lack of appropriate resources available to combat them make us wonder: will law enforcement, overextended and fighting increasingly impressive malware, be able to pursue ratters harassing families or sexexploiting other young people?

<sup>101</sup> A penetration test is a proactive and authorized attempt to evaluate the security of an IT infrastructure by safely attempting to exploit system vulnerabilities, including OS, service and application flaws, improper configurations, and even risky end-user behavior. - See more at: <http://www.coresecurity.com/penetration-testing-overview#sthash.DTr6WB9q.dpuf>

<sup>102</sup> <http://dwaterson.com/2013/04/14/a-rat-named-poison-ivy/>

<sup>103</sup> Grey hat hackers are a blend of both black hat and white hat activities. Often, grey hat hackers will look for vulnerabilities in a system without the owner’s permission or knowledge. If issues are found, they will report them to the owner, sometimes requesting a small fee to fix the issue.



## APPENDIX A: KNOWN ANTI-VIRUS IDENTIFIERS

Many of the anti-virus vendors have released updates to catch each RAT's signature. However, as new variants of RATs emerge, their signatures change as well. And some RATs are encrypted to hide from known anti-virus applications. You should always keep your system up-to-date to minimize the potential for infection.

Although there may be some anti-virus applications with signatures for RATs, detection is highly unlikely. RATs in Category III and Category IV are designed to either bypass anti-virus applications or close them when they start up. That doesn't mean you shouldn't update your system and your anti-malware application; it just means that this type of RAT does not usually target an individual, and if it did you would most likely not detect it.

Each Remote Access Trojan has a common name used in discussion. Also, each anti-virus vendor identifies these RATs by a unique name to that vendor. Some names of the Trojans were taken from other sites such as Virus Total ([www.virustotal.com](http://www.virustotal.com)) or from competing vendors from their virus encyclopedias.



## CATEGORY II IDENTIFIERS

| Common RAT Name <sup>102</sup>        | AVG Terminology                            | Kaspersky Terminology  | McAfee Terminology                                  | Panda Terminology            | Symantec Terminology  |
|---------------------------------------|--|--|---|------------------------------|---|
| <b>Adwind/<br/>UNRECOM</b>            | HackTool.AFIX                              | Trojan.Java.<br>Adwind.h   | BackDoor-FB-<br>FI!Adwind                           | Suspicious file              | PasswordRevealer  |
| <b>AndroRAT</b>                       | Atros.BC                                   | N/A  | RDN/Generic.<br>bfr!hw                              | N/A                          | Trojan.Gen.2  |
| <b>Back Orifice</b>                   | Backdoor.<br>BackOrifice                   | Backdoor.Win32.<br>BO2K.10                                       | RDN/Generic<br>BackDoor!xv                          | Backdoor Pro-<br>gram.LC     | N/A   |
| <b>Bifrost</b>                        | BackDoor.Pakes.B                           | Backdoor.Win32.<br>Bifrose.fsi                                   | BackDoor-CEP.<br>gen.cm                             | Generic Malware              | Backdoor.Bifrose  |
| <b>Blackshades<br/>(Black Shades)</b> | Worm/Generic3.<br>PUS; Dropper.<br>Msil.AD | Worm.Win32.<br>Shakblades.qmq;<br>HEUR:Trojan.<br>Win32.Generic  | RDN/Generic.<br>dx!dgl; RDN/Ge-<br>neric Dropper!vp | Trj/CI.A; Generic<br>Malware | W32.ShadeRat;<br>W32.ShadeRat.B;<br>W32.ShadeRat.C;<br>Trojan.Gen   |
| <b>Cerberus</b>                       | Autoit.DG                                  | Trojan-Dropper.<br>Win32.Agent.bpxo                              | Generic<br>Dropper!dgt                              | Trj/Autoit.gen               | N/A   |
| <b>DarkComet<sup>103</sup></b>        | Downloader.<br>Generic13.AWJB              | Backdoor.Win32.<br>DarkKomet.xyk;<br>Backdoor.Win32.<br>Fynloski | Generic BackDoor                                    | Trj/Packed.B                 | Backdoor.<br>Graybird   |
| <b>NanoCore</b>                       | BackDoor.<br>Generic18.ABLR                | Trojan.Win32.<br>Agent.apjvx;<br>HEUR:Trojan.<br>Win32.Generic   | RDN/Generic.<br>dx!dfv                              | Trj/CI.A                     | Trojan.Nancrat;<br>Trojan.Gen;<br>Suspicious.<br>Cloud.9;<br>Trojan.Mdropper;<br>Bloodhound.<br>Exploit.457 |

<sup>102</sup>Each Remote Access Trojan has a common name used in discussion. Also, each anti-virus vendor identifies these RATs by a unique name to that vendor. Some names of the Trojans were taken from other sites such as Total Virus ([www.virustotal.com](http://www.virustotal.com)) or from competing vendors (<http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=4487103&region=us>) from their virus encyclopedias.

<sup>103</sup>The creator of DarkComet has stopped developing new versions of the malware after seeing how the Syrian government used it against its own citizens. While it is no longer available for download, ratters who have earlier versions can still use it ([http://www.theregister.co.uk/2012/07/10/darkcomet\\_rat\\_killed\\_off/](http://www.theregister.co.uk/2012/07/10/darkcomet_rat_killed_off/)).



| Common RAT Name               | AVG Terminology   | Kaspersky Terminology                                 | McAfee Terminology                          | Panda Terminology         | Symantec Terminology        |
|-------------------------------|---|---|---|---------------------------|-----------------------------|
| <b>Poison Ivy (PoisonIvy)</b> | Win32/Agent.BB; Backdoor.PoisonIvy.AD; BackDoor Dorkbot; Backdoor.Generic | Backdoor.Win32.Poison.ckym; Backdoor.Win32.Poison.aec | Generic.bfr; Generic BackDoor; BackDoor-DIQ | Bck/Poison.E              | Backdoor.Darkmoon           |
| <b>njRAT</b>                  | PSW.ILUSpy (Trojan horse)   | Trojan.MSIL.Zapchast; HEUR:Trojan.Win32.Generic       | BackDoor-NJRat!0173B915E68B                 | Trj/CI.A; Generic Malware | Backdoor.Ratenjay           |
| <b>Sub7</b>                   | BackDoor.Generic12.OEN  | Backdoor.Win32.Jokerdoor                              | BackDoor-Sub7.svr                           | Bck/Sub7                  | Backdoor.SubSeven           |
| <b>Xtreme RAT</b>             | Dropper.Delf  | HEUR:Trojan.Win32.Generic                             | Generic BackDoor.zh                         | Generic Backdoor          | W32.Extrat; Backdoor.Trojan |



## CATEGORY III IDENTIFIERS

While individuals are unlikely to be targeted, and RATs in Categories III and IV are designed to bypass detection by anti-virus applications, we urge you to remain current with system updates and anti-malware applications.

| Common RAT Name <sup>104</sup> | AVG Terminology | Kaspersky Terminology           | McAfee Terminology       | Panda Terminology | Symantec Terminology  |
|--------------------------------|-----------------|---------------------------------|--------------------------|-------------------|---|
| <b>Carbanak</b>                | PSW.Agent.BEEE  | Trojan-PSW.<br>Win32.Agent.akql | RDN/Generic<br>PWS.y!bcr | Generic Malware   | Trojan.Carberp;<br>Trojan.Carberp.B;<br>Trojan.<br>Carberp.B!gm;<br>Trojan.Carberp.C; |
| <b>Dyre (Dyreza)</b>           | Generic_r.FEN   | Trojan-Banker.<br>Win32.Dyre.ms | Artemis!6E6A18C30FEC     | Trj/Genetic.gen   | Downloader.<br>Upatre;<br>Infostealer.<br>Dyranges                                    |
| <b>Kraken</b>                  | SHeur4.CGKA     | Trojan.Win32.<br>Fsysna.bfhv    | RDN/Generic.<br>dx!dj3   | Trj/Genetic.gen   | Trojan.Gen  |
| <b>Sir DoOom</b>               | N/A             | N/A                             | N/A                      | N/A               | N/A   |

<sup>104</sup>Each Remote Access Trojan has a common name used in discussion. Also, each anti-virus vendor identifies these RATs by a unique name to that vendor. Some names of the Trojans were taken from other sites such as Total Virus ([www.virustotal.com](http://www.virustotal.com)) or from competing vendors (<http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=4487103&region=us>) from their virus encyclopedias.



## CATEGORY IV IDENTIFIERS

While individuals are unlikely to be targeted, and RATs in Categories III and IV are designed to bypass detection by anti-virus applications, we urge you to remain current with system updates and anti-malware applications.

| Common RAT Name <sup>105</sup>     | AVG Terminology         | Kaspersky Terminology     | McAfee Terminology     | Panda Terminology  | Symantec Terminology   |
|------------------------------------|-------------------------|---------------------------|------------------------|--------------------|--|
| <b>Explosive</b>                   | VB2.AAVS (Trojan horse) | HEUR:Trojan.Win32.Generic | Generic BackDoor       | N/A                | Suspicious.Cloud.2   |
| <b>Regin</b>                       | BackDoor.Agent.AYVB     | Trojan.Win32.Regina       | Regin!sys              | Bck/Regin.A        | Backdoor.Regina  |
| <b>Trojan Laziok<sup>106</sup></b> |                         | Trojan.Win32.Fsysna.bfii  | RDN/Generic Dropper!wc | Generic Suspicious | Trojan.Laziok;<br>Trojan.Laziok!gm;<br>Backdoor.Cyberat;<br>Trojan.Zbot;<br>Trojan.Mdropper;<br>Bloodhound.<br>Exploit.457 |

<sup>105</sup>Each Remote Access Trojan has a common name used in discussion. Also, each anti-virus vendor identifies these RATs by a unique name to that vendor. Some names of the Trojans were taken from other sites such as Total Virus ([www.virustotal.com](http://www.virustotal.com)) or from competing vendors (<http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=4487103&region=us>) from their virus encyclopedias.

<sup>106</sup>IBID



## ACKNOWLEDGMENTS

Digital Citizens Alliance greatly appreciates the efforts of individuals and companies that have contributed to this publication. Without the efforts of all the cyber security companies and leaders, this report, and our privacy and data security would be in jeopardy.

Specifically, we'd like to thank these organizations for sharing their research publicly and answering our questions:

- **Symantec**
- **PandaLabs**

These individuals shared their expertise to help us understand some complicated issues:

- **Georgia Weidman**  
Founder of Bulb Security LLC and Shevirah
- **Luis Corrons-Granel**  
Technical Director of PandaLabs
- **Kevin Haley**  
Director of Product Management for Symantec Security Response
- **Greg Hanis**  
Founder of Global Network Protection
- **Gary Miliefsky**  
CEO of SnoopWall
- **Adam Rouse**  
Legal Fellow, Chicago-Kent College of Law

Long hours were spent on research for this report – gathering data, reviewing links, and explaining how things worked. Our thanks to:

- **Patrick Osborne**  
Principal, Outhaul Consulting, LLC

Also, when we needed to produce this report, we got help from talented professionals who shared special skills:

- **Nancy Shulins**  
Principal, Early Writer
- **Jennifer da Silva**  
Editor



digital **citizens**  
alliance 