1.1 OVERVIEW / Malicious actors seek to monetize the exfiltration and compromise of information from the computers and devices of their victims. The value of this information varies depending on the targeted victim’s reputation, level of income, place of work or membership in an organization. Several recent incidents covered by the mainstream media involved blackmail and extortion of the victims, some of whom were famous personalities.

The tools of choice in these incidents are Remote Access Tools (RATs), a type of software that can be used to control a device or computer remotely. When a RAT is installed unbeknownst to the targeted victim, it is called a Trojan horse or a Remote Administration Trojan, which also uses the RAT acronym.

The recent indictment and multiple arrests pertaining to the Blackshades RAT\(^1\) operation show that cyber criminals are seeking to extract sensitive information and targeting famous personalities\(^2\). RATs have also been used in advanced persistent threat (APT) campaigns, such as the use of XtremeRAT\(^3\) during the Molerat campaign.

In this threat advisory, PLXSert identifies and analyzes the most recent RAT threat, Blackshades RAT.

The list of options offered by the Blackshades RAT is enormous. A feature-packed RAT such as this can be very attractive to many cyber groups. It offers the ability to spy on victims while providing a malicious actor full and undisclosed access to their personal lives. Surveillance features such as webcam and screen capture provide tangible data about the victim, and keylog data can provide access to sensitive information. It also creates an avenue for attackers to hide their own malicious acts by using their victims as proxies, as well as offering mechanisms to use blackmail tactics for monetary or other personal gains.

1.2 RECENT HISTORY OF RATS / Remote access tools were not always used maliciously. The technology has been around for decades in the field of information technology, where companies and IT personnel sometimes require remote access to systems for troubleshooting purposes. In more recent years, however, RATs have been used maliciously to create back-doored systems in which an attacker can cause further harm to an infected system or systems at a later time.

---

\(^1\) "International Blackshades Malware Takedown," FBI, 19 May 2014.


\(^3\) Dahms, Timothy. "Molerats, Here for Spring!" FireEye Blog, 2 June 2014.
Significant anti-government campaigns have employed RATS and have been associated with APTs such as the Molerats campaign, where security firm Fireeye witnessed the propagation of XtremeRAT via email phishing campaigns⁴. RATs have been used to spy on officials and, likewise, government entities have used RATs to spy on their citizens.

DarkComet and Blackshades are among the most popular RATs in the criminal underground. DarkComet was allegedly developed by DarkCoderSC, an independent programmer and computer security specialist from France. Initially developed as a network administration tool, DarkComet quickly grew popular in the cybercrime world. It was even allegedly used by a major government entity to spy on rebels during a civil turmoil. This malicious use prompted the author to create the DarkComet RAT Remover, which he makes freely available.

The most recent RAT to make headlines is Blackshades, which is believed to have surfaced on the Internet in 2010. Blackshades RAT was allegedly a co-developed by Alex Yucel and Michael Hogue⁵; both were arrested recently by the FBI for their involvement in the creation and monetization of the Blackshades RAT⁶. U.S. officials have also announced the arrest of more than 90 other individuals allegedly connected to the Blackshades RAT operation.

Next, we dissect and investigate some of the capabilities and characteristics of the Blackshades toolkit.

1.3 INDICATORS / Blackshades RAT comes in two distinct versions: Blackshades NET and Blackshades Stealth. Blackshades NET was developed in Microsoft Visual Basic 6.0, while Blackshades Stealth was developed in Java. According to underground forum users, the NET version provides a wide range of options and utilizes a hardwareID lock feature to thwart software leakage and boost individual sales of the toolkit. In contrast, Blackshades Stealth uses encrypted communication, does not utilize a hardware ID lock, and provides fewer options.

Blackshades NET seems to be the more popular of the two and is the most accessible due to the availability of leaked and cracked versions that disable the hardware ID lock. The payload generated by the builder is also developed in Visual Basic, and can come in several different forms, depending on the options desired by the malicious actor.

The diversity of the Blackshades RAT also serves as its biggest weakness. The volume of options provided to its users creates more indicators of compromise, providing the security community with multiple options to identify and clean up a possible Blackshades infection.

⁵ Kenealy, Bill. "Feds Charge Blackshades Malware Makers with Computer Hacking." Business Insurance. 21 May 2014.
The following section will highlight some of the options provided by this toolkit. It can also serve as unique indicators for antivirus companies that wish to aid in the cleanup effort of Blackshades RAT infections.

**1.4 BLACKSHADES RAT ARCHITECTURE** / The typical architecture of a RAT consists of two components: a *client* and a *server*. When discussing RATs, the meanings of client and server are reversed; the server component resides on the infected host, and the client component is the command-and-control (C2) for the malicious actor.

The client component can be web-based or application-based depending on the implementation. Blackshades RAT uses an application-based C2, which an attacker uses as the central location to maintain and administer its botnet and to create bot payloads (also known as the builder). Once a victim has been successfully infected and a callback to the C2 has been established, the malicious actor has complete control over its victims. Figure 1 shows the main connection pane.

![Figure 1: The main connection pane of the Blackshades C2 with a list of infected hosts (one infected host in a lab environment)](image-url)
1.5 PAYLOAD CREATION / The Blackshades panel includes the capability to generate the infectious payload (server). The malicious actor has available several options to control the installation and persistence of the server executable. The Blackshades developers provide users with a full setup guide and table explaining some of the options to create the server payload. The table is shown in Figure 2 below.

<table>
<thead>
<tr>
<th>Box</th>
<th>Enter</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP/DNS</td>
<td>Your Host Name that you created on No-IP.com (yourhost.no-ip.biz) If you use more than one DNS, you can, just separate them with a colon e.g. DNS1:DNS2:DNS3 etc.</td>
</tr>
<tr>
<td>ConnectionPort</td>
<td>The port that the bot connects to. You may pick any number for this.</td>
</tr>
<tr>
<td>Transfer Port</td>
<td>3081</td>
</tr>
<tr>
<td>Server ID</td>
<td>A name to Identify your server, useful to Track it during spreading</td>
</tr>
<tr>
<td>Filename</td>
<td>What you want your server to be installed as. It will output your file as this but you can rename</td>
</tr>
<tr>
<td>Install Path</td>
<td>Where you want your server to be stored. App Data is better</td>
</tr>
<tr>
<td>Install Mode</td>
<td>Install – Copy the file to the directory; Melt – Delete file after it’s run; Protect process will not allow the process to be killed. Do NOT check any of these with .NET crypters!</td>
</tr>
<tr>
<td>Delay</td>
<td>How long after your server is run before it is installed (Tricks some AVs)</td>
</tr>
<tr>
<td>HKCU</td>
<td>The Registry entry for the server.</td>
</tr>
<tr>
<td>ActiveX</td>
<td>Press Generate a couple of times</td>
</tr>
<tr>
<td>Mutex</td>
<td>Press Generate a couple of times, prevents it from being run numerous times on one machine</td>
</tr>
<tr>
<td>Other</td>
<td>Infect USB – Helps with spreading; Compress – reduces server size; Change Icon – changes the server icon; Clone File Information – Makes your server appear to be a normal file.</td>
</tr>
</tbody>
</table>

Many of the options in this table are self-explanatory. However, a few offer unique capabilities, or are strong indicators of compromise. These are described in more detail below.

1.5a CLONE FILE / The Clone File option, listed under Other, allows an attacker to use the file information of another legitimate system program (or any other arbitrary program) and clone its information into the server payload for more stealth. In the lab environment, PLXSert was able to disguise a server payload with the file information from a legitimate executable, notepad.exe. Figure 3 illustrates this capability – the notepad executable is shown on the left, and the cloned version information (disguising the server payload) is shown on the right.
1.5b MUTEX / The mutex prevents multiple instances of the bot from running and infecting the same system, in the event an attacker accidentally attempts to re-infect current victims. The use of a mutex is a common technique among many families of malware to manage execution control. With the Blackshades RAT, a mutex may be randomly generated by the payload builder or an attacker may set a unique mutex for the payload manually.
1.5c .NET CRYPTER SETTINGS / This option provides the actor with default options for the file name and sets several default options to make the process of building the server payload straightforward with minimal user input. The name implies that these default settings allow attackers to use most crypters without conflict.

1.6 BLACKSHADES BUILDER / The Blackshades NET builder (shown in Figure 5 below) is straightforward. Its simplicity is one of the major reasons why this toolkit has gained so much popularity within the cybercrime community. Not only does it provide basic obfuscation features, it enables the malicious actor to manipulate the payload for more effective stealth and infection, depending on the host environment.

Figure 5: The bot builder for Blackshades NET
A feature not specific to Blackshades is the option to use FUD (Fully Undetectable) crypters. These programs can be used in conjunction with the builder to create an even more difficult to detect bot payload. FUD crypters are used to modify payloads in an effort to bypass popular anti-virus (AV) scanning engines. Cybercriminals have been known to test FUD crypter results on multi-AV engine websites such as VirusTotal to ensure their payloads avoid detection or have a low detection rate.

1.7 INFECTION AND PERSISTENCE / The Blackshades RAT server payload makes several system modifications in order to function properly. Most of these changes serve as the backbone for the tool’s capabilities. These system changes range from installing system-wide hooking procedures and monitoring keyboard and mouse data, to registry modifications that introduce persistence for the payload.

Once the Blackshades RAT server payload has infected a system, it typically goes through several stages of infection. One of the more important stages is stealth, where the RAT tries to leave the smallest footprint possible on the infected system. The next stage is establishing persistence, which allows the malware to survive system reboots. Once stealth and persistence are attained, a multitude of capabilities becomes available to the malicious actor.

1.7a REGISTRY MODIFICATIONS / The Windows registry is the single most-used artifact in any malware infection, and Blackshades RAT utilizes the Windows registry for several purposes. One purpose is ensuring the infection persists on the system during reboots. Another purpose is payload identification. Upon execution, the server payload adds keys to the registry to identify itself to the C2. A registry subkey with the name of the server is added under HKCU\Software\VB and VBA Program Settings\SrvID\ID. This location also contains the date the victim’s device was infected. Figure 6 below shows a screenshot of these registry entries.

![Figure 6: Identification data present in the Windows registry during a Blackshades RAT server infection](image)
Blackshades utilizes the Run key to maintain persistence on an infected system. This value may be modified by the malicious actor during bot creation and is typically located in any of the registry’s `Windows\CurrentVersion\Run` keys, as illustrated in Figure 7.

Another registry modification made by the Blackshades payload involves the Program Compatibility Assistant service. The Windows operating system (OS) provides this service to maintain application compatibility across different versions of the operating system. The Blackshades server utilizes this feature to force compatibility to the lowest supported OS version (Windows XP).

The payload also uses registry modifications to create firewall policies for itself, allowing the payload to connect back to the C2 without alerting the user about connection attempts.

![Figure 7: Windows registry entries installed by the server payload of Blackshades RAT](image)

![Figure 8: A server payload adding firewall policy exceptions for Blackshades RAT](image)
1.7b KEYBOARD AND MOUSE MONITORING / Blackshades uses the SetWindowsHookEx API to create system-wide hooks to monitor keyboard and mouse events. Figure 9 shows two hooks being placed by the Blackshades server payload, which are specific to system level hooks for monitoring keyboard (HookIdentifier 2) and mouse (HookIdentifier 7) events on the victim’s machine. More information about this API can be obtained from the MSDN webpage for the SetWindowsHookEx function.

![System-wide hooks](image)

Figure 9: System-wide hooks are placed on the victim's system for keyboard and mouse monitoring, as shown in a Cuckoo Sandbox report

1.7c ANTI-ANALYSIS TECHNIQUES / The Blackshades server payload implements anti-analysis features. It uses the IsDebuggerPresent() API to determine the presence of a debugger. It also contains an anti-kill feature that will automatically prompt the operating system to shut down if a user attempts to terminate the server payload process. This capability can be set by the malicious user during the bot-building process. In rare cases, attempting to kill the process can crash the operating system, resulting in the Windows blue screen of death.

![Anti-kill feature](image)

Figure 10: The anti-kill feature in the Blackshades RAT server process can cause the operating system to shut down if the user attempts to stop the malicious payload process
1.8 REMOTE ACCESS CAPABILITIES / The Blackshades RAT toolkit provides a malicious actor with a plethora of powerful remote access capabilities to control its victims. Once a victim has been infected, the level of compromise is high. These capabilities include system administration and modification, surveillance, system infection, networking controls and data exfiltration, as well as features that could be used for monetary gain.

1.8A SYSTEM ADMINISTRATION AND MODIFICATIONS / The Blackshades RAT provides operating system administration utilities such as process enumeration and access to the Windows registry. In the wrong hands, these utilities may cause irreversible damage to a compromised system. Malicious actors are capable of gathering the same information about a remote system as if they had physical access to the machine.

In addition, the malicious actor has the capability to download remote executables and run them on the infected machine. This functionality can be dangerous, allowing a malicious actor to propagate other malware, such as the Dirt Jumper DDoS toolkit called Drive or the Zeus crimeware toolkit.

Figure 11: System administration features provided by the Blackshades RAT panel
1.8b SURVEILLANCE / Blackshades has gained popularity primarily due to its surveillance features. The news media has reported their use against Miss Teen USA and by government entities during civil unrest. The Blackshades RAT toolkit allows malicious actors to monitor video and audio data on their infected victims. It also allows a malicious actor to record keylogging information from the user, potentially giving them access to sensitive credentials for banking, email, personal websites and other web-based applications.

The live logger is a keylogging feature that provides the cybercriminal with real-time logging data about its victim, including the window in use when inputting data and the victim's local time of day. These details give the criminal context about where the information is being used and for what purpose.

![Figure 12: The live logger interface as seen by a malicious actor](image)

Blackshades RAT also allows its users to capture the screen of an infected victim. This feature allows the attacker to watch what the user is doing in real time. The surveillance feature mimics the capabilities of legitimate software such as TeamViewer with the unfortunate advantage that its victims are unaware that they are sharing information.
1.8c ADDITIONAL FEATURES / The Blackshades RAT provides its users with several other features. For example, the Fun manager lets the malicious actor randomize a user’s mouse or display a message box to an infected victim. The Malware killer option is intended to clean the system of an infected payload, although this feature was ineffective in our own lab tests.

Figure 13: Miscellaneous features provided in the Blackshades RAT panel
1.8d REVENUE GENERATION / Other features may be used to generate revenue, such as *AD Clicker*, which allows an attacker to force the user to browse to certain webpages and systematically click ads. These ads are most likely placed by the malicious actor on self-hosted webpages. With a large enough botnet, this feature could result in ad revenue.

Blackshades RAT also includes *File hijacker* option that behaves like CryptoDefense and CryptoLocker ransomware, allowing an attacker to lock files on a system using a key-based cryptography scheme, and then prompting the victim to pay the key to unlock the files.

![Figure 14: The Blackshades file hijacker feature acts like ransomware](image-url)
1.9 NETWORK INDICATORS / Our initial analysis indicates the command protocol structure under an unencrypted connection is fairly simple. The Blackshades RAT uses specific default ports for communication. For example, the server payload uses port 3333 to establish a connection with the C2, and port 4444 is used for activities such as transferring files and using the screen capture feature. The Blackshades RAT client communicates to the server payload over port 3333 and sends its commands in the form of a letter (x) and then a sequence of numbers. These commands could be used as an indicator of compromise for the Blackshades RAT server payload on an infected system. Figure 15 shows some commands recorded while using some of the RAT's features.

Packet analysis revealed two unique packets that remained consistent across the entire connection. These appear to be the heartbeat or keepalive packets that notify the C2 of an established connection. The two packets can be identified by a series of x114.1.0 and x53.1.0 strings. Note that the keepalive and the command packets have a slight variation: a trailing period is appended to some (but not all) commands but is not found in the keepalive packets (Figure 16).
In addition to the normal traffic generated by the Blackshades RAT, malicious actors are also given the opportunity to anonymously surf the web through their infected victim’s connection by way of a proxy manager feature, which is shown in Figure 17. This feature allows the malicious actor to open up a port on the victim’s computer and redirect traffic through that IP address. This feature can be dangerous if used for cybercriminal activity as the activity may implicate an unsuspecting victim in a cybercrime.

![Figure 17: The proxy manager feature from the C2 in Blackshades RAT](image)

1.10 MITIGATION  / Blackshades RAT payloads can be difficult to detect, and therefore challenging to mitigate. Payloads may be customized and obfuscated using tools such as crypters. Furthermore, a typical infection consists of a multi-stage attack, where the victim is tricked into downloading a file, usually a dropper, which will subsequently download and execute the actual Blackshades payload.

Due to these effective infection techniques, enterprises and individuals must practice diligence while browsing the Internet, reading emails and using other web-based applications prone to drive-by attacks.

Antivirus companies have effectively identified the signatures of several variations of the Blackshades payload, and PLXSert provides a host-based YARA rule (Figure 18) for the identification of the payload. However, a malicious actor may customize the payload in a way that prevents detection with known signatures.
YARA is an open source tool designed to identify and classify malware threats. It is typically used as a host-based detection mechanism and provides a strong Perl Compatible Regular Expressions (PCRE) engine to match the identifying features of threats at a binary level. PLXsert uses YARA rules to classify the threats that persist across the campaigns and attacks that occur throughout the year. Figure 18 is a YARA rule provided by PLXsert to identify the Blackshades payloads identified in this advisory.

```
rule blackshadesNET
{
  meta:
    author = "PLXsert"
    filetype = "exe"
    date = "2014-06"
  strings:
    $s00="VBRUN" fullword
    $s01="BROWSER_FB" fullword
    $s02="PATH_WINLOGON" fullword
    $s03="TheBrowser_BeforeNavigate2" fullword
    $s04="TheBrowser_OnQuit" fullword
    $s05="BROWSER_FB_DocumentComplete" fullword
    $s06="BROWSER_FB_OnQuit" fullword
    $s07="FACEBOOK_START" fullword
    $s08="MSVBVM60.DLL" fullword
    $s09="MethodEngine" fullword
    $s10="strMutex" fullword
    $s11="AD_START" fullword
    $s12="PRINT_INSTRUCTIONS" fullword
    $s13="._vbaExceptionHandler" fullword
    $s14="ProcCallEngine" fullword

  condition:
    8 of ($s*)
}
```

Figure 18: The PLXsert YARA rule for the Blackshades RAT server payload

1.11 CONCLUSION / In attack campaigns, malicious actors switch and apply different attack vectors and customized tools to compromise their victims’ computers and devices. Stealth remote administration tools such as Blackshades RAT allow malicious actors to repurpose their botnets and require very little networking and operating systems knowledge.

The large number of features combined with its ease-of-use has helped Blackshades RAT flourish among aspiring cybercriminals and even more seasoned malicious actors. It has gained the interest of major organized crime groups and government entities. The FBI’s takedown of the official webpage and subsequent mass arrests are a testament to the popularity of the toolkit itself.7

PLXsert expects the Blackshades RAT toolkit will gain more traction and continue to be a persistent threat for motivated cyber criminals. PLXsert will continue to monitor the use of Blackshades RAT and provide updates when applicable.

The Prolexic Security Engineering and Research Team (PLXsert) monitors malicious cyber threats globally and analyzes these attacks using proprietary techniques and equipment. Through research, digital forensics and post-event analysis, PLXsert is able to build a global view of security threats, vulnerabilities and trends, which is shared with customers and the security community. By identifying the sources and associated attributes of individual attacks, along with best practices to identify and mitigate security threats and vulnerabilities, PLXsert helps organizations make more informed, proactive decisions.

Akamai® is a leading provider of cloud services for delivering, optimizing and securing online content and business applications. At the core of the company’s solutions is the Akamai Intelligent Platform™ providing extensive reach, coupled with unmatched reliability, security, visibility and expertise. Akamai removes the complexities of connecting the increasingly mobile world, supporting 24/7 consumer demand, and enabling enterprises to securely leverage the cloud. To learn more about how Akamai is accelerating the pace of innovation in a hyperconnected world, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 40 offices around the world. Our services and renowned customer care enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers and contact information for all locations are listed on www.akamai.com/locations

©2014 Akamai Technologies, Inc. All Rights Reserved. Reproduction in whole or in part in any form or medium without express written permission is prohibited. Akamai and the Akamai wave logo are registered trademarks. Other trademarks contained herein are the property of their respective owners. Akamai believes that the information in this publication is accurate as of its publication date; such information is subject to change without notice. Published 07/14.