Lobshot

Threat: **Remote Access Trojan**

Author: **Jeffrey Farnan** Date Originally Published: **May 30th, 2023**

1. SUMMARY

- A new malware called Lobshot was recently discovered which infects Windows devices and is distributed using Google ads. The malware impersonates legitimate software but has a feature called hVNC (Hidden Virtual Network Computing) which allows attackers to access a victim's windows device without been noticed. Lobshot appears to be leveraged for financial purposes employing banking trojans and info-stealing capabilities.

2. MALWARE FAMILY

- **Type** = RAT (Remote Access Trojan).
- **Sub-type** = Infostealer.

- **Remote Access Trojan:** Lobshot's notable feature revolve around its ability to remotely access the compromised host via an hVNC module and stealthily perform actions on it without attracting the victim's attention.
- **Infostealer:** Lobshot is used to find financial information such as credit card details, crypto wallet data or steal account passwords.

3. MALWARE CHARATERISTICS

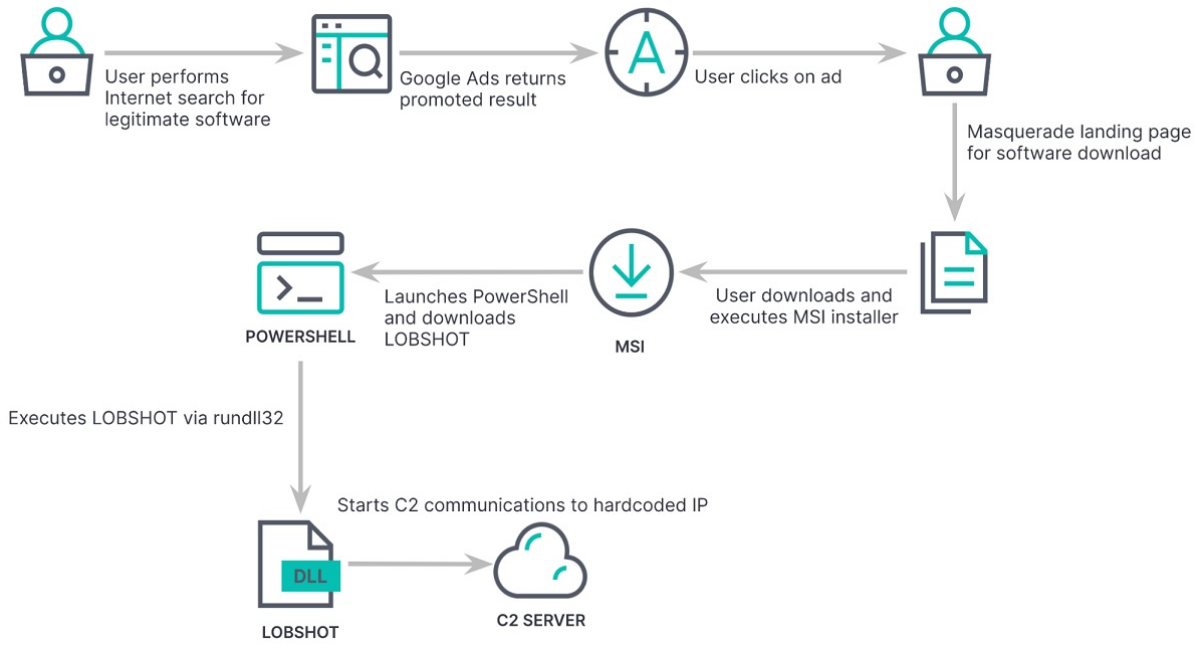
- **Suspected country of origin** = Russia.
- **First seen date/period** = July 2022.
- **Still active** = Yes.
- **Last submitted sample as of writing this article** = May 18th, 2023.

4. MALWARE HISTORY

- Lobshot malware is developed by the Russian cybercrime group TA505 , this group is also referred to as Evil Corp and active since 2014. This group is known for operating the Dridex trojan and ransomware families such as Locky, Bart, BitPaymer, WastedLocker and Necurs campaigns. Lobshot has been operating since 2022 with more than 500 unique samples observed since July last year.

5. MALWARE DESCRIPTION

- This infection chain begins with a user performing an Internet search for legitimate software (e.g., AnyDesk). However, one of the search results that the user clicks on is a Google Ad, which leads the user to a masquerading landing page for the software download. There has been a dramatic increase int threat actors using Google Ads to distribute malware in search results. These advertising campaigns impersonated websites for 7-ZIP, VLC, OBS, Notepad++, CCleaner, TradingView, Rufus, and many more applications.
- An example would be a malicious ad promoting the AnyDesk remote application which was found circulating on the Google search engine. The landing pages looked very similar to that of the original website and included a 'Download Now' button. Once the users clicked on the button, it launched the execution of the LOBSHOT malware.
- Lobshot deploys a hVNC module or hidden virtual network computing software modified to control a hidden desktop on the infected device rather than the main desktop used by the victim. This allows the threat actor to remotely control a Windows desktop computer without the victim knowing about it. The attackers can gain full remote control of the infected device, allowing them to execute a wide range of malicious activities. Overall, LOBSHOT can cause significant damage to a victim's computer and put their sensitive information at risk.



- The hVNC (Hidden Virtual Network Computing) component offers a number of core capabilities such as direct and unobserved access to the machine. It continues to be effective in bypassing fraud detection systems and is often built into many popular families as a plugin.
- After being executed, the malware will verify whether Microsoft Defender is active or not. If it finds that the Defender is active, it will immediately stop its execution to avoid getting detected.
- It will extract information about the infected device, such as the currently running processes, and transmit it to the attacker's server.
- After Lobshot finishes executing, it moves a copy of itself to the C:\ProgramData folder, spawning a new process using explorer.exe. This way, it terminates the original process and deletes the original file.

- The attackers behind LOBSHOT can perform various actions on an infected device by issuing commands to start a new explorer[.]exe process, opening a Run command window, launching a browser, changing system settings, modifying sound settings, accessing the clipboard, and more. Lobshot can also change its command-and-control server and update itself.
- Lobshot malware can be used for a variety of other malicious activities such as employing banking trojans, etc.

6. POTENTIAL CUSTOMER DEFENSE

- Like most malware Lobshot gets installed by user interaction. Be cautious about downloading and installing software from unknown sources and especially free versions. Only download software and files from reputable sources.
- Be wary of suspicious email attachments, links or pop-ups and always avoid clicking on them.
- Be sure to keep your operating system and all software up to date with the latest security patches and updates.
- Use a reputable antivirus or security software and keep it up to date. If you believe that your computer is already infected, it is recommend running a scan with an Antivirus for Windows to automatically eliminate infiltrated malware.

Research Sources:

- https://www.pcrisk.com/removal-guides/26621-lobshot-malware
- https://www.bleepingcomputer.com/news/security/new-lobshot-malware-gives-hackers-hidden-vnc-access-to-windows-devices/
- https://thehackernews.com/2023/05/lobshot-stealthy-financial-trojan-and.html
- https://www.securityweek.com/new-lobshot-hvnc-malware-used-by-russian-cybercriminals/
- https://www.securityweek.com/new-lobshot-hvnc-malware-used-by-russian-cybercriminals/
- https://heimdalsecurity.com/blog/new-lobshot-malware-deployed-via-google-ads/