Drokbk Malware Uses GitHub as Dead Drop Resolver

Counter Threat Unit Research Team ⋮⋮ 12/9/2022

By: Counter Threat Unit Research Team

Secureworks® Counter Threat Unit™ (CTU) researchers are investigating the Drokbk malware, which is operated by a subgroup of the Iranian government-sponsored COBALT MIRAGE threat group. This subgroup is known as Cluster B. Drokbk is written in .NET and is made up of a dropper and a payload. The malware has limited built-in functionality and primarily executes additional commands or code from the command and control (C2) server. Early signs of its use in the wild appeared in a February 2022 intrusion at a U.S. local government network. A Drokbk malware sample was not available from that incident for analysis, but CTU™ researchers later discovered samples uploaded to the VirusTotal analysis service.

Drokbk is deployed post-intrusion alongside other access mechanisms as an additional form of persistence within the victim's environment. COBALT MIRAGE's preferred form of remote access uses the Fast Reverse Proxy (FRPC) tool. While COBALT MIRAGE Cluster A uses a modified version of this tool known as TunnelFish, Cluster B favors the unaltered version. The only public mention of Drokbk.exe is in a March third-party report describing activity that exhibits signs of a Cluster B intrusion. In that instance, the malware used the C2 domain activate-microsoft . cf, which is known to be associated with Cluster B.

The February intrusion that Secureworks incident responders investigated began with a compromise of a VMware Horizon server using two Log4j vulnerabilities (CVE-2021-44228 and CVE-2021-45046). Forensic artifacts indicated Drokbk.exe was extracted from a compressed archive (Drokbk.zip) hosted on the legitimate transfer . sh online service. The threat actors extracted the file to C:\Users\DomainAdmin\Desktop\ and then executed it.

The Drokbk dropper checks for the existence of the c:\programdata\SoftwareDistribution directory and creates the directory if it does not exist. The dropper then writes all bytes from an internal resource to c:\users\public\pla. This is a temporary step; the extracted file (pla) is then copied to c:\programdata\SoftwareDistribution\SessionService.exe. Using this newly created file, the dropper adds the SessionManagerService service for persistence. Finally, the dropper deletes c:\users\public\pla. Figure 1 illustrates the installation process. CTU researchers have observed that the Cluster B operators favor c:\users\public\ as a directory used across multiple malware tools.

Figure 1. Process tree for Drokbk installation. (Source: Secureworks)

SessionService.exe is the main malware payload, and it begins by finding its C2 domain. A C2 domain is often preconfigured in malware. However, Drokbk uses the dead drop resolver technique to determine its C2 server by connecting to a legitimate service on the internet (e.g., GitHub). The C2 server information is stored on a cloud service in an account that is either preconfigured in the malware or that can be deterministically located by the malware.

Figure 2 shows decompiled .NET code from SessionService.exe. The binary uses the GitHub API to search for the 'mainrepositorytogeta' repository.

Figure 2. DnSpy-decompiled .NET code from SessionService.exe. (Source: Secureworks)

This code identifies the specific GitHub account and the request used to locate the malware's C2 server. The response is stored within the README.md file hosted on the GitHub account (see Figure 3). In this campaign, the threat actor used a GitHub account with the username Shinault23.

Figure 3. Code used to locate the C2 server within a GitHub account. (Source: Secureworks)

This approach gives the threat actors a degree of resiliency against shuttering of their GitHub account, as they can create a new account with a matching repository name. It also allows the malware to dynamically update its C2 server by repeating this process.

The first commit to the README.md file occurred on June 9, 2022, suggesting this campaign began around this date. Between June 9 and July 13, the threat actors changed the C2 server multiple times. GitHub maintains a commit history for the file, listing each change (see Figure 4).
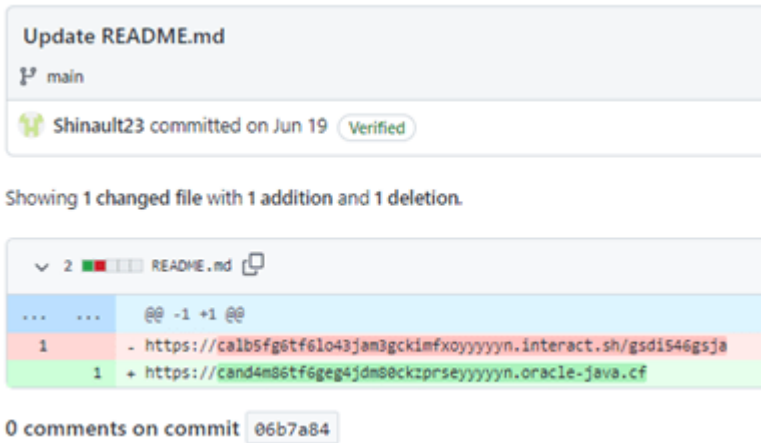
Figure 4. Example of the commit history for the Shinault23 account. (Source: Secureworks)

Figure 5 lists the C2 servers configured between June 9 and July 13. These domain names and URL structures align with infrastructure patterns observed in other Cluster B activity, providing additional evidence supporting technical attribution.

Figure 5. List of Drokbk C2 servers from the README.md file. (Source: Secureworks)

Using the information from README.md, SessionService.exe sends an initial request to the C2 server. The request contains the hostname and current time (see Figure 6).
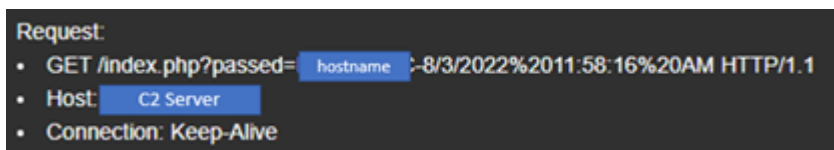
Figure 6. Sandbox output showing initial Drokbk beacon. (Source: Secureworks)

During execution, CTU researchers observed Drokbk creating the following files. No payloads or commands were received from the C2 during analysis.

- C:\Windows\Temp\v2ggla
- C:\Windows\Temp\vdoma434
- C:\programdata\Interop Services

To mitigate exposure to this malware, CTU researchers recommend that organizations use available controls to review and restrict access using the indicators listed in Table 1. Note that IP addresses can be

reallocated. The domains, IP addresses, and URL may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
372b1946907ab9897737799f3bc8c131 00519705	SHA1 hash	Drokbk.exe malware
e26a66bfe0da89405e25a66baad95b05	MD5 hash	Drokbk.exe malware
4eb5c832ce940739d6c0eb1b4fc7a78d ef1dd15e	SHA1 hash	Drokbk.exe malware
64f39b858c1d784df1ca8eb895ac7eaf 47bf39acf008ed4ae27a796ac90f841b	SHA256 hash	Drokbk.exe malware
8c8e184c280db126e6fcfcc507aea925	MD5 hash	Drokbk.exe malware
aefab35127292cbe0e1d8a1a2fa7c39c 9d72f2ea	SHA1 hash	Drokbk.exe malware
29dc4cae5f08c215d57893483b5b42cb 00a2d0e7d8361cda9feeaf515f8b5d9e	SHA256 hash	Drokbk.exe malware
14a0e5665a95714ff4951bd35eb73606	MD5 hash	Drokbk malware payload (SessionService.exe)
0426f65ea5bcff9e0dc48e236bbec293 380ccc43	SHA1 hash	Drokbk malware payload (SessionService.exe)
a8e18a84898f46cd88813838f5e69f05 240c4853af2aee5917dcee3a3e2a5d5a	SHA256 hash	Drokbk malware payload (SessionService.exe)
b90f05b5e705e0b0cb47f51b985f84db	MD5 hash	Fast Reverse Proxy used by COBALT MIRAGE Cluster B
5bd0690247dc1e446916800af169270f 100d089b	SHA1 hash	Fast Reverse Proxy used by COBALT MIRAGE Cluster B
28332bdbfaeb8333dad5ada3c10819a1 a015db9106d5e8a74beaaf03797511aa	SHA256 hash	Fast Reverse Proxy used by COBALT MIRAGE Cluster B
activate-microsoft.cf	Domain name	Drokbk C2 server
dns-iprecords.tk	Domain name	Drokbk C2 server
oracle-java.cf	Domain name	Drokbk C2 server
51.89.135.154	IP address	Hosts COBALT MIRAGE domain (oracle-java.cf)
142.44.149.199	IP address	Drokbk C2 server
142.44.149.199/gsdi546gsja	URL	Drokbk C2 server
universityofmhealth.biz	Domain name	Drokbk C2 server
142.44.198.202	IP address	Drokbk C2 server

Table 1. Indicators for this threat.