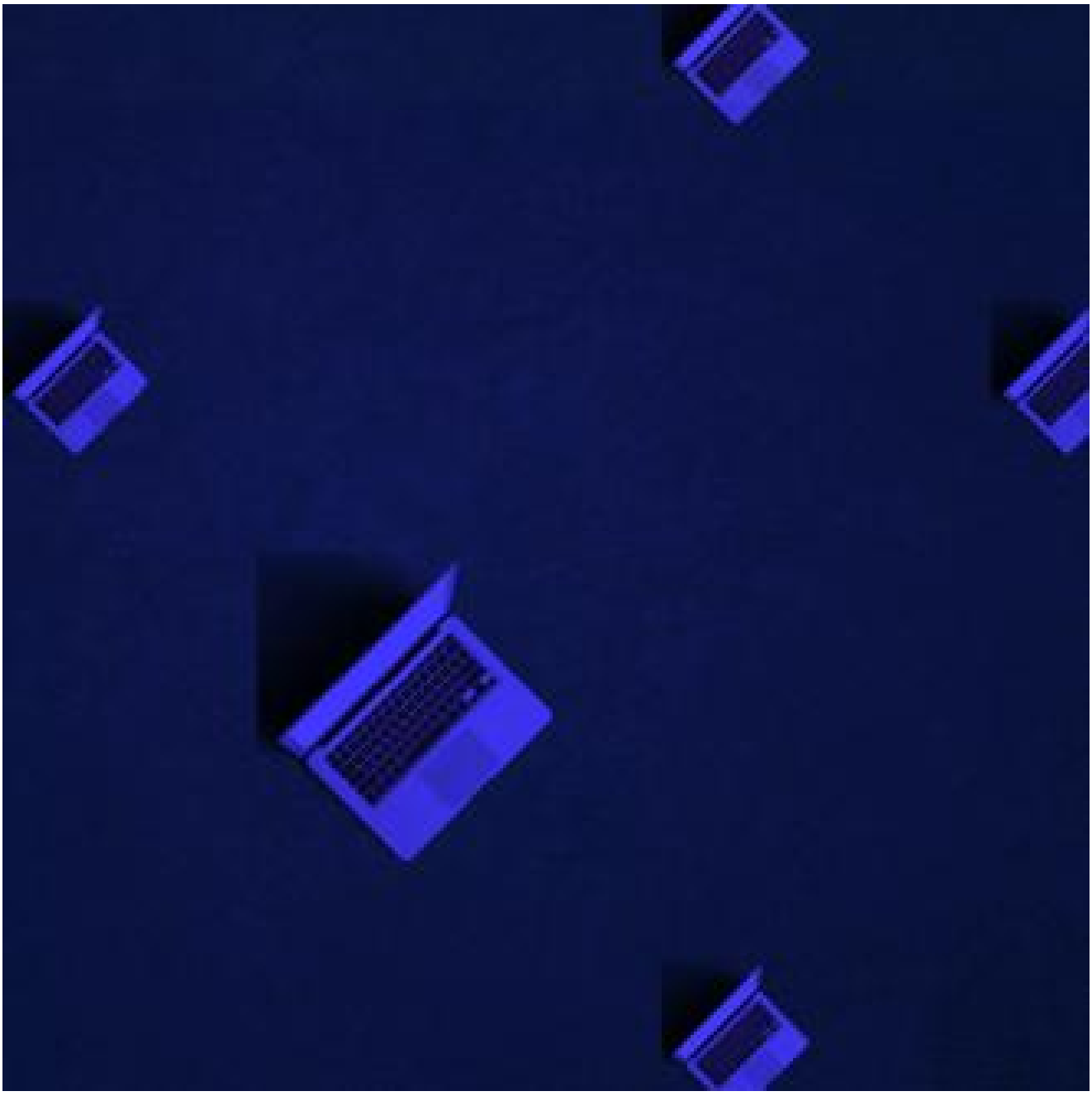
Law Enforcement Takes Down Qakbot

secureworks.com/blog/law-enforcement-takes-down-qakbot



On August 29, 2023, U.S. law enforcement announced a takedown of the Qakbot criminal botnet (also known as Qbot). The financially motivated GOLD LAGOON threat group has operated the Qakbot malware since 2007. The modular malware supports numerous capabilities, including facilitating ransomware attacks.

Secureworks® Counter Threat Unit™ (CTU) researchers tracking the Qakbot botnet observed the technical takedown operation. At 23:27 UTC on August 25, CTU™ researchers detected the Qakbot botnet distributing shellcode to infected devices. The shellcode unpacks a custom DLL (dynamic link library) executable that contains code that can cleanly terminate the running Qakbot process on the host.

The DLL uses a clever method that involves sending a QPCMD_BOT_SHUTDOWN instruction via a named pipe that Qakbot uses to send and receive messages between processes on the host. Qakbot pipe names are generated using a pseudorandom algorithm that the DLL uses to generate the correct name for the system it is running on. The DLL then calls CallNamedPipeA and sends the QPCMD_BOT_SHUTDOWN instruction to the pipe (see Figure 1).

```
*v8 = 0x30004;                          // QPCMD_BOT_SHUTDOWN 0x4
v8[1] = 0;
generate_guid(Buffer, a1 + 3);
lpNamedPipeName = lstrcat("\\\\.\\pipe\\");   // \\\\.\\pipe\\{23814566-A2ED-5AB2-B3B2-92851CA1D4DF}
if ( !lpNamedPipeName )
  return 0;
if ( hHeap )
  lpOutBuffer = HeapAlloc(hHeap, 8u, 0x208u);
else
  lpOutBuffer = 0;
BytesRead = 0;
if ( CallNamedPipeA(lpNamedPipeName, lpInBuffer, lpInBuffer[1] + 8, lpOutBuffer, 0x208u, &BytesRead, 0x1388u)
  && *lpOutBuffer != 10 )
{
```

Figure 1. Custom DLL generating the pipe name and sending the QPCMD_BOT_SHUTDOWN command. (Source: Secureworks)

Qakbot has a PipeServer() function that can send and receive messages between processes that it has injected into (e.g., receiving data stolen from a web browser via the STAGER_1 module). There are seven PipeServer() commands (see Table 1).

Command number	Name
1	QPCMD_EXEC_COMMAND
4	QPCMD_BOT_SHUTDOWN
6	QPCMD_GET_STAGER_1_BODY_MAIN
7	QPCMD_GET_STAGER_1_BODY_MAIN_SIZE
8	QPCMD_GET_STAGER_1_BODY_UPDATE
14	QPCMD_GET_STAGER_1_TYPE
9	QPCMD_GET_STAGER_1_BODY_UPDATE_SIZE

Table 1. PipeServer() commands.

When the QPCMD_BOT_SHUTDOWN command (command number 4) is received, the 'keep_alive' global variable is set to 1 (see Figure 2).

```
if ( *(_WORD *)v3 == 4 )
{
  sub_1000C05E("PipeServer(): QPCMD_BOT_SHUTDOWN", v19);
  sub_10012D62(0, 0);
  v1 = 1;
  keep_alive = 1;
  v26 = 1;
}
```

Figure 2. Qakbot setting keep_alive to 1 after QPCMD_BOT_SHUTDOWN. (Source: Secureworks)

When this global variable is set to 1, the Qakbot main thread stops running and the Qakbot process exits (see Figure 3).

```
while ( !keep_alive )
{
  sub_1000EB84(&dword_10035E90);
  sub_10004155(v1, v1);
  sub_1000C05E("qbot_main_thread() working tBotStartTime=%llu now_time=%llu", dword_10035E68[0]);
  (*(void (__stdcall **)(int))(dword_10035E00 + 196))(4000);
}
sub_100068BB();
sub_1000C05E("qbot_main_thread(): ===>>> stopping threads...", v3);
sub_10013AC2();
sub_10007943();
sub_1000C05E("qbot_main_thread(): ===>>> Finished. ret=%d", 0);
return 0;
```

Figure 3. Qakbot terminating if keep_alive is 1. (Source: Secureworks)

Qakbot establishes persistence on a host when it detects a user initiating a system shutdown. Using the named pipe to terminate the Qakbot process bypasses persistence. As a result, Qakbot will not run if the host is restarted.

CTU researchers have long maintained visibility of Qakbot's backend infrastructure. At approximately the same time as the DLL began neutralizing infections, CTU researchers observed GOLD LAGOON's backend infrastructure had stopped responding and some infrastructure had been replaced. To interact with infected hosts, the replacement servers required a certificate that can sign messages. It appears that the certificates were obtained and used for good intentions.

The unresponsiveness of GOLD LAGOON's infrastructure and the distribution of payloads to terminate Qakbot processes indicated takedown efforts. These robust efforts should reduce the number of infected hosts and hinder GOLD LAGOON's attempts to regain control of the botnet.

- **Tags:**
- Blog
- Research

Back to all Blogs