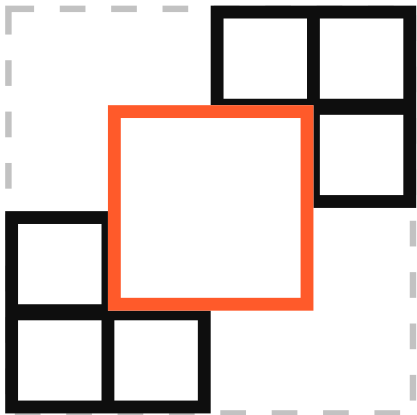


BLUERABBIT: A Golang-Based Backdoor with Ransomware...



A full-featured backdoor with file encryption, drive wiping, and a C2 channel that looks like normal message broker traffic. Meet BLUERABBIT, this Golang-based backdoor, attributed to a likely Iran-nexus threat actor, routes its command-and-control through RabbitMQ (AMQP) for tasking, Redis for state management, and MinIO for S3-compatible data exfiltration. It is a full-spectrum intrusion tool: remote access, system profiling, file encryption with a .candy extension, and two distinct disk-wiping modules capable of rendering systems permanently unrecoverable.

First observed in mid-to-late March 2026, BLUERABBIT is suspected of targeting entities in Israel. According to the Google Threat Intelligence Group (GTIG), the malware is related to the same likely Iran-nexus activity cluster that previously leveraged BLUEWIPE and SEWERGOO in June 2025. Symbols were left intact in the analyzed sample, revealing that the binary was known internally as “Rabbit” and compiled as a developmental build.

The background material for this analysis is the GTIG report 26-10016354, available at [VirusTotal](#).

Attack Flow

The following sequence represents BLUERABBIT’s operational kill chain as observed in analysis. Each stage maps to a dedicated section of this report.

#	Phase	Description
1	Initial Execution	Binary executes, checks HKCU\Software\OneDrive\Environment registry key for prior execution
2	Persistence	Creates “OneDrive Update” scheduled task with 60-second repeat interval and startup trigger
3	C2 Registration	Connects to RabbitMQ (AMQP), declares a queue named after the victim device

4	Tasking	Receives numeric task IDs over AMQP, maps each to a built-in module
5	Reconnaissance	Profiles OS, hardware, network, installed software, security products, BitLocker status, drivers, domain
6	Exfiltration	Stages files in GUID-named directories, exfiltrates to attacker-controlled MinIO infrastructure
7	Destructive Actions	Disables recovery, encrypts files (.candy), and/or wipes disks across all logical drives

Capability Matrix

BLUERABBIT operates on a modular tasking system. The C2 server sends a numeric task ID, and the malware maps it to one of over a dozen built-in modules. The table below summarizes the core capability categories.

Category	Description
Remote Access	Full remote desktop-style control with keyboard and mouse input via VNC; shell command execution
Surveillance	Screenshot capture, screen recording, process and Windows service enumeration and management
System Profiling	OS details, hardware configuration, network settings, installed software, security products, BitLocker status, installed drivers, domain information
File Exfiltration	Files staged in GUID-named directories and exfiltrated to attacker-controlled MinIO (S3-compatible) cloud storage
File Encryption	Encrypts files across all logical drives with .candy extension; replaces desktop wallpaper with AI-generated "High-Alert" image
Disk Wiping (Single-Pass)	Overwrites all drives with random data in a single pass
Disk Wiping (Multi-Pass)	Writes zeros, random data, and 0xFF in sequence across all drives, rendering systems permanently unrecoverable

Anti-Recovery	Disables automatic reboot, system recovery, and scheduled maintenance; takes ownership of critical boot files
----------------------	---

The combination of exfiltration and encryption is consistent with a double extortion model: data is stolen before encryption occurs. This means data has already left the network before a victim even knows they are compromised, and paying a ransom does not guarantee the data will not be leaked or sold.

Initial Execution and Persistence

Upon execution, BLUERABBIT checks the registry key HKCU\Software\OneDrive\Environment to track its execution count. If this key does not exist, the malware assumes it is running for the first time and executes a PowerShell command to establish persistence as a scheduled task named “OneDrive Update,” deliberately impersonating a legitimate Microsoft service.

The task is configured with two triggers: one that fires five seconds after registration with a one-minute repeat interval, and one at system startup. It runs at the highest privilege level available to the compromised user, has no execution time limit, and restarts automatically up to three times on failure. The observed PowerShell persistence command is as follows:

```
powershell -Command "
    $action = New-ScheduledTaskAction -Execute
    'C:\Users\testname\Downloads\SupportAssistance_exe\SupportAssistance.exe' -Argument '-
    ExecutionPolicy Bypass -WindowStyle Hidden'
    $trigger1 = New-ScheduledTaskTrigger -Once -At ((Get-Date).AddSeconds(5)) -
    RepetitionInterval (New-TimeSpan -Minutes 1)
    $trigger2 = New-ScheduledTaskTrigger -AtStartup
    $Principal = New-ScheduledTaskPrincipal -UserId
    ([System.Security.Principal.WindowsIdentity]::GetCurrent().Name) -LogonType S4U -RunLevel
    Highest
    $settings = New-ScheduledTaskSettingsSet -StartWhenAvailable -DontStopOnIdleEnd -
    AllowStartIfOnBatteries -DontStopIfGoingOnBatteries -Hidden -RestartCount 3 -RestartInterval
    (New-TimeSpan -Minutes 1) -ExecutionTimeLimit (New-TimeSpan -Days 0)
    Register-ScheduledTask -TaskName 'OneDrive Update' -Action $action -Trigger @($trigger1,
    $trigger2) -Principal $Principal -Force -Settings $settings | Out-Null
    Start-ScheduledTask -TaskName 'OneDrive Update'
"
```

The -ExecutionPolicy Bypass -WindowStyle Hidden arguments passed to the malware binary appear to be unused, as these are PowerShell flags that have no effect when passed directly to a non-PowerShell executable. The authors also did not strip symbols from the binary, which significantly aided analysis. Configuration parameters such as C2 server IPs, ports, and authentication credentials are, however, protected with AES encryption.

Because the task repeats every 60 seconds with automatic restart on failure, simply killing the BLUERABBIT process is insufficient. The scheduled task itself must be removed to break persistence.

Command-and-Control Infrastructure

BLUERABBIT’s main execution loop follows the sequence MessageReader, ProcessTask, UpdateRedis, relying on enterprise messaging and database protocols rather than conventional HTTP-based C2. This architecture uses three distinct channels, each serving a specific operational purpose:

Protocol	Technology	Function
AMQP	RabbitMQ	Primary tasking channel. Malware declares a queue named after the victim device; consumer tag is the full path to the malicious executable. Task IDs received as JSON.
RESP	Redis	Results and task state written back after module execution.
S3 (HTTP)	MinIO	S3-compatible channel for large file exfiltration to attacker-controlled cloud storage.

When launching the VNC remote desktop module, BLUERABBIT creates a firewall rule under the deceptive name Microsoft.Windows.CloudExperienceHost to blend in with legitimate Windows components.

Temporary staging directories are generated using a GUID-like naming scheme where characters are drawn from the full alphanumeric range rather than hexadecimal only. This is a meaningful detection signal: legitimate Windows GUIDs are strictly hexadecimal (0–9, A–F), so the presence of characters G–Z in a GUID-formatted directory name is anomalous and hutable. The path for files staged for exfiltration is written to the registry key HKCU\Software\OneDrive\ProfileConfig.

Destructive Actions Preparation

Prior to executing destructive actions, BLUERABBIT uses takeown and icacls to take ownership of and grant full access to critical boot files, including bootmgr, ntoskrnl.exe, and winload. The following registry modifications are made to disable automatic reboot and system recovery:

Registry Path	Value	Effect
HKLM\SYSTEM\CurrentControlSet\Control\CrashControl	AutoReboot = 0	Prevents automatic reboot on crash
HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	NoAutoRebootWithLoggedOnUsers = 1	Blocks reboot while users are logged on
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Maintenance	MaintenanceDisabled = 1	Disables scheduled maintenance

HKLM\SYSTEM\CurrentControlSet\Control\Windows	NoAutoRebootWithLoggedOnUsers = 1	Additional reboot suppression
HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	AlwaysAutoRebootAtScheduledTime = 0	Disables forced scheduled reboot

The raw commands, preserved here for detection engineering purposes:

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\CrashControl /v AutoReboot /t REG_DWORD /d 0 /f
reg add HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU /v
NoAutoRebootWithLoggedOnUsers /t REG_DWORD /d 1 /f
reg add HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Maintenance /v
MaintenanceDisabled /t REG_DWORD /d 1 /f
reg add HKLM\SYSTEM\CurrentControlSet\Control\Windows /v NoAutoRebootWithLoggedOnUsers /t
REG_DWORD /d 1 /f
reg add HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU /v
AlwaysAutoRebootAtScheduledTime /t REG_DWORD /d 0 /f
```

Collectively, these modifications ensure that once BLUERABBIT begins encryption or wiping, the system cannot automatically recover, reboot into repair mode, or interrupt the destructive process.

Detection Opportunities

Several characteristics of BLUERABBIT create reliable detection opportunities that defenders can operationalize:

- **Non-hex GUID directories:** BLUERABBIT's staging directories use the full alphanumeric range (A–Z, 0–9) in a GUID-formatted path. Legitimate Windows GUIDs are strictly hexadecimal. Any GUID-formatted folder containing characters G–Z is anomalous and worth investigating.
- **Scheduled task fingerprint:** The combination of a task named "OneDrive Update," created via New-ScheduledTaskAction with AllowStartIfOnBatteries, Hidden, and an immediate start trigger, is distinctive and unlikely to appear in legitimate enterprise tooling.
- **AMQP/RabbitMQ traffic:** On endpoint devices, externally routed AMQP traffic is a high-fidelity detection signal. However, in environments where RabbitMQ is part of the production stack, defenders should also baseline expected broker connections and alert on anomalous destinations or authentication patterns.
- **MinIO command-line artifacts:** The MinIO client (mc) executed with `alias set --insecure` or performing S3-style operations from non-server endpoints should be treated as suspicious. Defenders should also monitor for mc spawned by non-standard parent processes: if mc is being called by something other than a shell session, cron job, or known automation tooling (e.g., spawned by an application binary, a scripting engine like python or powershell, or an unusual service), that's a strong indicator of programmatic misuse consistent with automated exfiltration or staging.
- **Boot file ownership changes:** Any process running `takeown` or `icacls` against `bootmgr`, `ntoskrnl.exe`, or `winload.efi/winload.exe` outside of a sanctioned patching window should trigger an immediate alert.

Indicators of Compromise

Type	Indicator
File (SHA-256)	633d4cbd496b1094495da89a64f5e6c31a0f6d4d1488411db5b0cba1cfe42001
File (SHA-256)	9706a192e2c1a1faaf0a521daf31c2af60ff4590e3f47bbb4abc227f42af0683
File (SHA-256)	ce9ad5f6c12019f4aae5b189bd8ddf5bb09e75b06a0a587b25a855c65948c913
File (SHA-256)	f622ed85ef31ad4ab973f4e74524866fe1bb44f0965ad2b2ad796cd657a05bfd
IP Address	185.182.193.21
IP Address	212.8.248.104
JA3	806dab5164cf60d94026b88ab2d9851d
JA4	t13i131000_f57a46bbacb6_e5728521abd4
JA3	d80125b9429e9d5f06ace959f00de8d0
JA3S	d75f9129bb5d05492a65ff78e081bcb2
JA4	t13i130900_f57a46bbacb6_e7c285222651

BLUERABBIT represents a capable and operationally mature threat. Its use of enterprise protocols for C2, modular architecture, and dual-purpose destructive capability signal an adversary that is investing in tooling designed for high-impact operations. For organizations concerned about exposure to Iran-nexus threats, the detection opportunities and indicators above provide an immediate starting point for proactive hunting.

ARC Labs will continue to track this activity cluster and publish updates as the threat evolves.