Cuba Ransomware Group's New Variant Found Using Optimized Infection Techniques

trendmicro.com/en_us/research/22/f/cuba-ransomware-group-s-new-variant-found-using-optimized-infect.html

June 8, 2022

Cuba ransomware is a malware family that has been seasonally detected since it was first observed in February 2020. It resurfaced in November 2021 based on the FBI's official notice, and has reportedly attacked 49 organizations in five critical infrastructure sectors, amassing at least US$ 43.9 million in ransom payments.

We observed Cuba ransomware's resurgence in March and April this year. Our monitoring showed that the malware authors seem to be pushing some updates to the current binary of a new variant. The samples we examined in March and April used BUGHATCH, a custom downloader that the malicious actor did not employ in previous variants specifically for the staging phase of the infection routine.

In late April we also noticed another variant of the ransomware, this time targeting two organizations based in Asia. This blog entry focuses on our analysis of the latest samples uncovered from this period.

While the updates to Cuba ransomware did not change much in terms of overall functionality, we have reason to believe that the updates aim to optimize its execution, minimize unintended system behavior, and provide technical support to the ransomware victims if they choose to negotiate.

Our analysis of the new variant revealed that the malicious actor added some processes and services to terminate the following:

- MySQL
- MySQL80
- SQLSERVERAGENT
- MSSQLSERVER
- SQLWriter
- SQLTELEMETRY
- MSDTC
- SQLBrowser
- sqlagent.exe
- sqlservr.exe
- sqlwriter.exe
- sqlceip.exe
- msdtc.exe
- sqlbrowser.exe
- vmcompute
- vmms
- vmwp.exe
- vmsp.exe
- outlook.exe
- MSExchangeUMCR
- MSExchangeUM
- MSExchangeTransportLogSearch
- MSExchangeTransport
- MSExchangeThrottling
- MSExchangeSubmission
- MSExchangeServiceHost
- MSExchangeRPC
- MSExchangeRepl
- MSExchangePOP3BE
- MSExchangePop3

- MSExchangeNotificationsBroker
- MSExchangeMailboxReplication
- MSExchangeMailboxAssistants
- MSExchangeIS
- MSExchangeIMAP4BE
- MSExchangeImap4
- MSExchangeHMRecovery
- MSExchangeHM
- MSExchangeFrontEndTransport
- MSExchangeFastSearch
- MSExchangeEdgeSync
- MSExchangeDiagnostics
- MSExchangeDelivery
- MSExchangeDagMgmt
- MSExchangeCompliance
- MSExchangeAntispamUpdate
- Microsoft.Exchange.Store.Worker.exe

```
int sub_401907()
{
  HANDLE v0; // eax@1
  HANDLE TokenHandle; // [sp+8h] [bp-20h]@1
  struct _TOKEN_PRIVILEGES NewState; // [sp+Ch] [bp-1Ch]@2
  struct _LUID Luid; // [sp+1Ch] [bp-Ch]@2

  v0 = GetCurrentProcess();
  if ( OpenProcessToken(v0, 0x28u, &TokenHandle) )
  {
    LookupPrivilegeValueA(0, "SeDebugPrivilege", &Luid);
    NewState.Privileges[0].Luid = Luid;
    NewState.PrivilegeCount = 1;
    NewState.Privileges[0].Attributes = 2;
    AdjustTokenPrivileges(TokenHandle, 0, &NewState, 0x10u, 0, 0);
  }
  sub_4029D0(L"MySQL", 0xFFFFFFFF);
  sub_4029D0(L"MySQL80", 0xFFFFFFFF);
  sub_4029D0(L"SQLSERVERAGENT", 0xFFFFFFFF);
  sub_4029D0(L"MSSQLSERVER", 4u);
  sub_4029D0(L"SQLWriter", 0xFFFFFFFF);
  sub_4029D0(L"SQLTELEMETRY", 0xFFFFFFFF);
  sub_4029D0(L"MSDTC", 0xFFFFFFFF);
  sub_4029D0(L"SQLBrowser", 0xFFFFFFFF);
  sub_40297D(L"sqlagent.exe");
  sub_40297D(L"sqlservr.exe");
  sub_40297D(L"sqlwriter.exe");
  sub_40297D(L"sqlceip.exe");
  sub_40297D(L"msdtc.exe");
  sub_40297D(L"sqlbrowser.exe");
  sub_4029D0(L"vmcompute", 4u);
  sub_4029D0(L"vmms", 4u);
  sub_40297D(L"vmwp.exe");
  sub_40297D(L"vmsp.exe");
  sub_40297D(L"outlook.exe");
  sub_4029D0(L"MSExchangeUMCR", 0xFFFFFFFF);
  sub_4029D0(L"MSExchangeUM", 0xFFFFFFFF);
  sub_4029D0(L"MSExchangeTransportLogSearch", 0xFFFFFFFF);
  sub_4029D0(L"MSExchangeTransport", 0xFFFFFFFF);
```

Figure 1. Screenshot of the list of processes and services that the Cuba ransomware seeks to terminate

Another apparent change is the expansion of the safelisted directories and file extensions that it will avoid encrypting:

Directory Safelist:

- \windows\
- \program files\microsoft office\
- \program files (x86)\microsoft office\
- \program files\avs\
- \program files (x86)\avs\

- \$recycle.bin\
- \boot\
- \recovery\
- \system volume information\
- \msocache\
- \users\all users\
- \users\default user\
- \users\default\
- \temp\
- \inetcache\
- \google\

Extension Safelist:

- .exe
- .dll
- .sys
- .ini
- .lnk
- .vbm
- .cuba

```
dd offset aWindows      ; DATA XREF: sub_40122F:loc_40126F↑r
                        ; "\\windows\\"
dd offset aProgramFilesMi ; "\\program files\\microsoft office\\"
dd offset aProgramFilesX8 ; "\\program files (x86)\\microsoft office"...
dd offset aProgramFilesAv ; "\\program files\\avs\\"
dd offset aProgramFiles_0 ; "\\program files (x86)\\avs\\"
dd offset aRecycle_bin  ; "\\$recycle.bin\\"
dd offset aBoot         ; "\\boot\\"
dd offset aRecovery     ; "\\recovery\\"
dd offset aSystemVolumeIn ; "\\system volume information\\"
dd offset aMsocache     ; "\\msocache\\"
dd offset aUsersAllUsers ; "\\users\\all users\\"
dd offset aUsersDefaultUs ; "\\users\\default user\\"
dd offset aUsersDefault ; "\\users\\default\\"
dd offset aTemp         ; "\\temp\\"
dd offset aInetcache    ; "\\inetcache\\"
dd offset aGoogle       ; "\\google\\"
dd 'EDIF'               ; DATA XREF: sub_401ED4+15↑r
```

Figure 2. Array of directories it excludes from encryption

We compared the new variant used in late April 2022 to the previous ones and found that the former did not have all the commands or functions that came with the latter. The malicious actors only retained two commands in the new one that are directory- or location-related phrases. These are as follows:

- local
- network

Notably, the wording of the ransom note used in the latest variant (see Figure 4) is different from the previous one that the malicious actors used in the samples we analyzed in March this year, but the onion site indicated in both ransom notes is the same. The ransom note used in late April 2022 explicitly states that they will publish exfiltrated data on their Tor site if the victims refuse to negotiate after three days, an apparent use of the double extortion technique. The ransomware gang did not clearly state the threat of publication of stolen data in the ransom note dropped in March 2022 (see Figure 3).

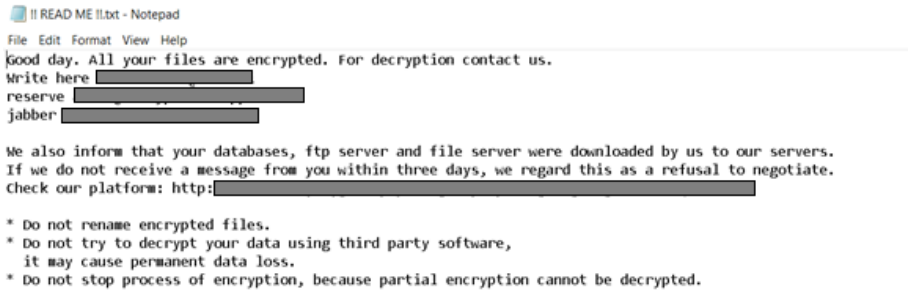

Figure 3. Cuba ransomware's ransom note retrieved from samples that we analyzed in March 2022

Another new feature of the latest ransom note is the addition of quTox, a means for technical support to the ransomware victims to facilitate ransom payment negotiation.

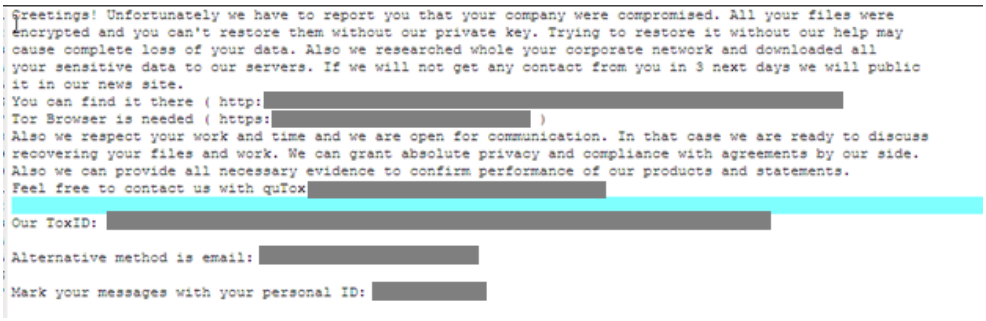

Figure 4. Cuba ransomware's ransom note retrieved from samples analyzed in late April 2022, with mention of quTox as technical support to facilitate ransom payment negotiations

We are still investigating the latest set of samples and have yet to establish the entire infection chain for the new Cuba ransomware variant. As mentioned, the indicators that were commonly seen in most of the recent infections were not present in the latest samples we saw. Moreover, our detections of new samples in May suggest that Cuba ransomware's attacks will persist in the coming months, possibly with more updates to the malware that are par for the course.

Recommendations

As new malware variants emerge, a proactive cybersecurity stance is important to ensure that organizations are protected against modern ransomware threats. To defend systems against similar attacks, organizations can establish security frameworks that systematically allocate resources based on an enterprise's needs.

Consider following the security frameworks established by the Center of Internet Security and the National Institute of Standards and Technology when developing your own cybersecurity strategies. The frameworks they created help security teams to mitigate risks and minimize exposure to threats. Implementing the best practices discussed in their respective frameworks can save organizations the time and effort when they customize their own. Their frameworks guide organizations through the whole process of planning while providing suggestions on measures that need to be established first.

Indicators of Compromise (IOCs)

SHA256	Trend Micro Detection
89288de628b402621007c7ebb289233e7568307fb12a33aac7e834504c17b4af	Ransom.Win32.BACUCRYPT.YPCD2T

Trend Micro Research observed the resurgence of the Cuba ransomware group that launched a new malware variant using different infection techniques compared to past iterations. We discuss our initial findings in this report.

By: Don Ovid Ladores June 08, 2022 Read time: (words)

Content added to Folio