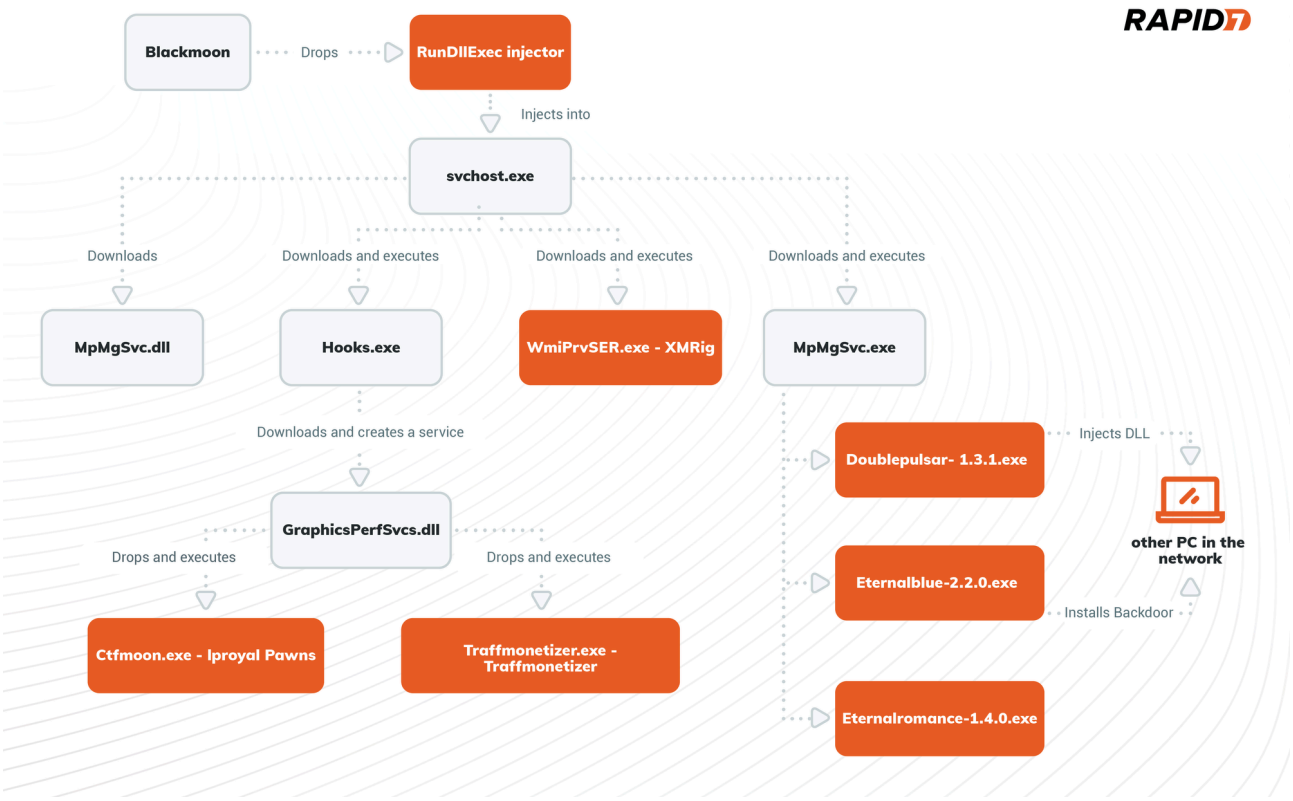
Old Blackmoon Trojan, NEW Monetization Approach

By Natalie Zargarov

Published: 2023-07-13 · Archived: 2026-04-05 21:19:34 UTC

Rapid7 is tracking a new, more sophisticated and staged campaign using the Blackmoon trojan, which appears to have originated in November 2022. The campaign is actively targeting various businesses primarily in the USA and Canada. However, it is not used to steal credentials, instead, it implements different evasion and persistence techniques to drop several unwanted programs and stay in victims' environment for as long as possible.

Blackmoon, also known as KRBanker, is a banking trojan first spotted in late September 2015 when it was used to target banks of the Republic of Korea. Back in 2015, it employed a "pharming" technique to steal credentials from targeted victims. This technique involved redirecting traffic to a forged website when a user attempts to access one of the banking sites being targeted by the cyber criminals. The fake site masquerades as the original site and urges visitors to submit their information and credentials.



Stage 1 - Blackmoon

The Blackmoon trojan was named after a debug string "blackmoon," that is present in its code:

Blackmoon string found inside malware's code

Blackmoon drops a dll into C:\Windows\Logs folder named RunDllExe.dll and implements a Port Monitor persistence technique. Port Monitors are related to the Windows Print Spooler Service or spoolsv.exe. When adding a printer Port Monitor, a user (or the attacker in our case) has the ability to add an arbitrary dll that acts as the monitor. There are two ways to add a Port Monitor: via Windows Registry for persistence or via a AddMonitor API call for immediate dll execution.

Our sample implements both, it calls AddMonitor API to immediately execute RunDllExe.dll:

AddMonitorA API call

It also sets a driver value in HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors\RunDllExe registry key to the malicious dll path.

Driver value set under monitors registry key

Next, the malware adds a shutdown system privilege to the Spooler service by adding SeShutdownPrivilege to the RequiredPrivileges value of HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Spooler registry key.

RequiredPrivileges data before and after the update

The malware disables Windows Defender by setting HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware value to “1”.

It also stops and disables “Lanman” service (the service that allows a computer to share files and printers with other devices on the network).

To block all incoming RPC and SMB communication the malware executes the set of following commands:

```
 netsh ipsec static add policy name=Block
netsh ipsec static add filterlist name=Filter1
netsh ipsec static add filter filterlist=Filter1 srcaddr=any dstaddr=Me dstport=135 protocol=TCP
netsh ipsec static add filter filterlist=Filter1 srcaddr=any dstaddr=Me dstport=135 protocol=UDP
netsh ipsec static add filter filterlist=Filter1 srcaddr=any dstaddr=Me dstport=139 protocol=TCP
netsh ipsec static add filter filterlist=Filter1 srcaddr=any dstaddr=Me dstport=139 protocol=UDP
netsh ipsec static add filter filterlist=Filter1 srcaddr=any dstaddr=Me dstport=445 protocol=TCP
netsh ipsec static add filter filterlist=Filter1 srcaddr=any dstaddr=Me dstport=445 protocol=UDP
netsh ipsec static add filteraction name=FilteraAtion1 action=block
netsh ipsec static add rule name=Rule1 policy=Block filterlist=Filter1 filteraction=FilteraAtion1
netsh ipsec static set policy name=Block assign=y
```

The malware sets two additional values under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\aspnet_staters: Work and Mining, both set to "1".

Next, the malware checks if one of the following services exists on the victim's computer:

- clr_optimization_v3.0.50727_32
- clr_optimization_v3.0.50727_64
- WinHelpsvcs
- Services
- Help Service
- KuGouMusic
- WinDefender
- Msubridge
- ChromeUpdater
- MicrosoftMysql
- MicrosoftMssql
- Conhost
- MicrosotMaims
- MicrosotMais

If the service is found, it will be disabled (by setting "Start" value under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\servicename to "4") or deleted by using the DeleteService API call.

The malware enumerates running processes by using a combination of CreateToolhelp32Snapshot and Process32First and Process32Next API calls to terminate the service's process (if one is running).

Finally, a Powershell command is executed to delete the running process' file and the malware exits.

Stage 2 - RunDllExe.dll - injector

RunDllExe.dll is executed by Spooler service and is responsible for injecting a next stage payload into the newly executed svchost.exe process. The malware implements Process Hollowing injection technique. The injected code is a C++ file downloader.

Stage 3 - File Downloader

The downloader first checks if 'Work' and 'Mining' values exist and are set under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\aspnet_staters registry key, if the values do not exist, it will create them and set both to "1".

This part of the attack flow checks if all the necessary downloaded files are present (by using PathFileExistsA API call) on the PC, if not, the malware sleeps for two minutes before every download and then uses the URLDownloadToFileA API call to download the following files:

- C:\WINDOWS\Temp\MpMgSvc.dll
- C:\WINDOWS\Temp\Hooks.exe
- C:\WINDOWS\Temp\MpMgSvc.exe
- C:\Windows\Microsoft.NET\Framework\v3.0\WmiPrvSER.exe

After the download, all files except MpMgSvc.dll are executed:

Execution tree

Stage 4 - Hook.exe - dropper

Hook.exe drops an additional dll to the user's roaming folder C:\Users\Username\AppData\Roaming\GraphicsPerfSvcs.dll and creates a new service named GraphicsPerfSvcs, which will be automatically executed at system startup. The service's name is almost identical to the legitimate service named GraphicsPerfSvc, which belongs to the graphics performance monitor service. Naming services and files similarly to those that exist on the victim's OS is an evasion technique widely used by threat actors.

Malicious Service under the legitimate one

The dropper then starts the created service. It creates and executes a .vbs, which is responsible for deleting Hook.exe and the .vbs itself:

Created .vbs

Stage 4.1 - MpMgSvc.exe - spreader MpMgSvc.exe first creates a new \BaseNamedObjects\Brute_2022 mutex. As it is responsible for spreading the malware, it drops Doublepulsar-1.3.1.exe, Eternalblue-2.2.0.exe, Eternalromance-1.4.0.exe and all required file libraries into the C:\Windows\Temp folder.

Then, it scans the network for PC's with open 3306, 445, 1433 ports. If any open ports are found, the spreader will attempt to install a backdoor by using EternalBlue and send shellcode to inject dll with Doublepulsar as implemented in the Eternal-Pulsar github project .

Eternal-Pulsar commands in spreader memory

There are two dlls dropped, one for x64 architecture and the second one for x86. When injected by Doublepulsar, it will download the first stage Blackmoon malware and follow the same execution stages described in this analysis.

Stage 4.2 - WmiPrvSER.exe - XMRig miner

WmiPrvSER.exe is a classic XMRig Monero miner. Our sample is the XMRig version 6.18, and it creates a BaseNamedObjects\\Win__Host mutex on the victim's host. You can find a full report on XMRig here.

Stage 5 - GraphicsPerfSvcs service - dropper

As mentioned in the previous stage, the GraphicsPerfSvcs service will be started automatically at system startup. Every time it runs, it will check if two of the following files exist:

- C:\Windows\TEMP\ctfmoon.exe
- C:\Windows\Microsoft.NET\traffmonetizer\Traffmonetizer.exe

If not found, it will drop both those files and all needed dlls for their execution.

The dropper also creates two new firewall rules that allow all outbound connections from dropped files by executing the following commands:

- netsh advfirewall firewall add rule name=ctfmoon dir=out program=C:\Windows\Microsoft.NET\ctfmoon.exe action=allow
- netsh advfirewall firewall add rule name=traffmonetizer dir=out program=C:\Windows\Microsoft.NET\traffmonetizer\traffmonetizer.exe action=allow

Ctfmoon.exe firewall rule creation

The service stays up and constantly attempts to read from the URL: hxxp://down.ftp21[.]cc/Update.txt. At the time of the analysis, this URL was down so we were not able to observe its content. However, following the service code, it seems to read the URL content and check if it contains one of the following commands:

[Delete File], [Kill Proccess], or [Delete Service], which will delete file, kill process or delete service accordingly.

Stage 6 - Ctfmoon.exe and Traffmonetizer.exe - Traffic Stealers

GraphicsPerfSvcs service executes two dropped files: Ctfmoon.exe and Traffmonetizer.exe**,** both appeared to be Potentially Unwanted Programs (PUP's) in the form of traffic stealers. Both are using the "network bandwidth sharing" monetization scheme to make "passive income".

Ctfmoon.exe is a cli version of the Iproyal Pawns application. It gets the user email address and password as execution parameters to associate the activity and collect the money to the passed account. GraphicsPerfSvcs executes the following command line to start Iproyal Pawns: ctfmoon.exe -email=usax138@protonmail.com -password=123456Aa. -device-name=Win32 -accept-tos

We can see that the user mentioned in our execution parameters already made $169:

Iproyal Pawns earnings from our sample

The Traffmonetizer.exe is similar to Ctfmoon.exe, created by Traffmonetizer. It reads the user account data from a settings.json file dropped in users roaming directory. Our .json file contains the following content:

{"Token":"1gUgURMzQiuGFgttIdjeZBS0G6fqFlVvhCKlqzfHd3o=","StartWithWindows":false,"Accepting":true}.

Conclusion

The analysis in this blog reveals the efforts threat actors put into the attack flow, by using several evasion and persistence techniques as well as different approaches to make passive income using victims' resources.

MITRE ATT&CK Techniques:

Persistence	Boot or Logon Autostart Execution: Port Monitors (T1547.010)	The Blackmoon trojan (a95737adb2cd7b1af2291d143200a82d8d32 a868c64fb4acc542608f56a0aeda) is using the Port Monitor technique to establish persistence on the target host.
Persistence	Create or Modify System Process: Windows Service (T1543.003)	The Hook.exe dropper (1A7A4B5E7C645316A6AD59E26054A95 654615219CC03657D6834C9DA7219E99F) creates a new service to establish persistence on the target host.
Defense Evasion	Process Injection: Process Hollowing (T1055.012)	The dll dropped by Blackmoon (F5D508C816E485E05DF5F58450D623DC6B FA35A2A0682C238286D82B4B476FBB) is using the Process Hollowing technique to evade endpoint security detection.
Defense Evasion	Impair Defenses: Disable or Modify Tools (T1562.001)	The Blackmoon trojan (a95737adb2cd7b1af2291d143200a82d8 d32a868c64fb4acc542608f56a0aeda) disables Windows Defender to evade end-point security detection.
Lateral Movement	Exploitation of Remote Services (T1210)	The MpMgSvc.exe spreader (72B0DA797EA4FC76BA4DB6AD131056257965D F9B2BCF26CE2189AF3DBEC5B1FC) uses EternalBlue and DoublePulsar to spread in organization's environment.
Discovery	Network Share Discovery (T1135)	The MpMgSvc.exe spreader (72B0DA797EA4FC76BA4DB6AD131056257965D F9B2BCF26CE2189AF3DBEC5B1FC) scans the network to discover open SMB ports.
Impact	Resource Hijacking (T1496)	The XMRing miner (ECC5A64D97D4ADB41ED9332E4C0F5DC7DC02 A64A77817438D27FC31C69F7C1D3), Iproyal Pawns ctfmoon.exe (FDD762192D351CEA051C0170840F1D8D

		171F334F06313A17EBA97CACB5F1E6E1) and Traffmonetizer trafficStealer (2923EACD0C99A2D385F7C989882B7CCA 83BFF133ECF176FDB411F8D17E7EF265) are executed to use victims' resources.
Impact	Service Stop (T1489)	The Blackmoon trojan (a95737adb2cd7b1af2291d143200a82d8d 32a868c64fb4acc542608f56a0aeda) stops updates and security products services.
Command and Control	Application Layer Protocol: Web Protocols (T1071.001)	The downloader (E9A83C8811E7D7A6BF7EA7A656041BCD68968 7F8B23FA7655B28A8053F67BE99) downloads the next stage payloads over the HTTP protocol. GraphicsPerfSvcs service (5AF88DBDC7F53BA359DDC47C3BCAF3F5FE 9BDE83211A6FF98556AF7E38CDA72B) uses HTTP protocol to get command from C&C server.

IOC's

File name	**SHA-256**	
445.exe	a95737adb2cd7b1af2291d143200a82 d8d32a868c64fb4acc542608f56a0aeda	Blackmoon Trojan
RunDllExe.dll	F5D508C816E485E05DF5F58450D623DC 6BFA35A2A0682C238286D82B4B476FBB	Injector
Injected code	E9A83C8811E7D7A6BF7EA7A656041BCD 689687F8B23FA7655B28A8053F67BE99	Downloader
MpMgSvc.dll	E9BD4A9C6EA27033BCB696E65D7441DC2D 42CD7F9F02084B5C704316F0A4FDDF	
Hooks.exe	1A7A4B5E7C645316A6AD59E26054A95654615 219CC03657D6834C9DA7219E99F	Dropper
MpMgSvc.exe	72B0DA797EA4FC76BA4DB6AD131056257965 DF9B2BCF26CE2189AF3DBEC5B1FC	Spreader
WmiPrvSER.exe	ECC5A64D97D4ADB41ED9332E4C0F5DC7DC02 A64A77817438D27FC31C69F7C1D3	XMRig
GraphicsPerfSvcs.dll	5AF88DBDC7F53BA359DDC47C3BCAF3F5FE9BDE 83211A6FF98556AF7E38CDA72B	Dropper

File name	SHA-256	
Doublepulsar-1.3.1.exe	15FFBB8D382CD2FF7B0BD4C87A7C0BFFD1541C2FE86865AF445123BC0B770D13	Shellcode installer
Eternalblue-2.2.0.exe	85B936960FBE5100C170B777E1647CE9F0F01E3AB9742DFC23F37CB0825B30B5	Exploit
Eternalromance-1.4.0.exe	B99C3CC1ACBB085C9A895A8C3510F6DAAF31F0D2D9CCB8477C7FB7119376F57B	Exploit
X64.dll	275A9A7B99F3474CBF8A61964A6022E3CF7BAF76E0EE2FBA31A708D8F1E25BD0	shellcode
X86.dll	F247A48D3ECDBDF91FCD7A2D8728ADAAF06149586ADDE62DE7212C6DE645AD58	shellcode
Ctfmoon.exe	FDD762192D351CEA051C0170840F1D8D171F334F06313A17EBA97CACB5F1E6E1	Iproyal Pawns
Traffmonetizer.exe	2923EACD0C99A2D385F7C989882B7CCA83BFF133ECF176FDB411F8D17E7EF265	Traffmonetizer
usax138@protonmail.com		Iproyal Pawns account
1gUgURMzQiuGFgttIdjeZBS0G6fqFlVvhCKlqzfHd3o=		Traffmonetizer token
hxxp://down.ftp21[.]cc		C&C server

References

- https://posts.slayerlabs.com/monitor-persistence/
