BADAN SIBER DAN SANDI NEGARA

Jalan Harsono R.M. Nomor 70, Ragunan, Pasar Minggu, Jakarta Selatan 12550
Telepon (021) 7805814, Faksimile (021) 78844104
***Website* : https://bssn.go.id, *E-mail* : humas@bssn.go.id**

INDICATOR OF COMPROMISE QILIN RANSOMWARE

RILIS: 15 APRIL 2025

No	*Files*	*MD5*	*Remarks*
Remote IP			
1	180[.]131[.]145[.]73		
2	184[.]174[.]96[.]70		
C2			
1	hxxps://misctoolsupdate[.]com/fr		
2	hxxps://login.misctoolsupdate[.]com/fr		
3	hxxps://login.misctoolsupdate[.]com/ch		
4	hxxps://misctoolsupdate[.]com/mt		
5	hxxps://sso.misctoolsupdate[.]com/ch		
7	hxxps://misctoolsupdate[.]com/mt		
8	hxxps://sso.misctoolsupdate[.]com/be		
9	hxxps://misctoolsupdate[.]com/be		
Email			
1	nopaperplanes@proton[.]me		
Binaries			
1	C:\Users\xxx\Downloads\realtekapo2.dll	B377FF706FB36006CDB1B6B71E62B7E4	HEUR:Trojan.Win32.Cobalt.vho
2	C:\ProgramData\BigFix\Remote Control\realtekapo2.dll		
3	C:\Users\xxx\Downloads\vmdns.exe	D2E1D5CE8B85D5E5F42106B28C3F6E1E	HEUR:Trojan.Win32.Cobalt.vho

No	*Files*	*MD5*	*Remarks*
4	C:\Windows\2bd2e97.exe	F51B82D0BA1B46CF56C9BCC82127FB45	HEUR:Trojan.Win32.Cobalt.vho
5	C:\Windows\9f53d2c.exe	28B19B7E689C339912793FCA5627541E	VHO:Trojan.Win32.Agent.gen
6	C:\Windows\system32\runonce.exe	01F892412F9AD5027D6E8A19ECF530FE	MEM:Trojan-PSW.Win32.Mimikatz.gen
7	C:\Windows\System32\dllhost.exe	D2AB39EA2C0FCD172751F84BDA723A97	MEM:Trojan.Win64.Cobalt.gen
8	5081fc9.exe	BE0529FAA555736DBF72D88CB50CB318	
9	C:\Users\xxx\Desktop\Advanced IP Scanner 2.5.3850.exe	52E666A32D0847B416B66AD9AA98BBED	
10	C:\Windows\System32\RuntimeBroker.exe	D63063C53168E4EA8235EEE65EDEA4E6	MEM:Trojan.Multi.Cobalt.gen
11	vm.dll	B377FF706FB36006CDB1B6B71E62B7E4	
Cache (CobaltStrike)			
1	C:\Users\xxx\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_00000f	D2E1D5CE8B85D5E5F42106B28C3F6E1E	HEUR:Trojan.Win32.Cobalt.vho
2	C:\Users\xxx\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\D9131116D41AFD79AB84432377FC614D	A3CBB5F2990496C85B4F6ABAB004A371	HEUR:Trojan.Win32.Cobalt.vho
3	C:\Users\xxx\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Datalf_000010	3F8B9190CB67E64F86E82FEB6F959F9B	HEUR:Trojan.Win32.Cobalt.vho
4	C:\tmp\9392.exe	5C1350F8FC2A2A57B5C5C109B4E05975	HEUR:Trojan.Win32.Cobalt.vho
5	rclone.exe	1BF171B1F388691C3985DF6FB6C3F0D1	
6	C:\ProgramData\rs64c.exe	D1C43F8DB230BDF18C61D672440EBA12	

No	*Files*	*MD5*	*Remarks*
7	C:\Windows\system32\runonce.exe (SharpHound)	71D6E59EE15E5B30D7FF1B561E683F45	
8	C:\ProgramData\20250321160217 BloodHound.zip	FF1CB06659DA3EC3C76622F7A4E9AB39	
9	C:\Windows\431f9cc.exe	AD395D2D9C5FDD78A355CBF5AB65FA62	
10	C:\Windows\9517238.exe	7D77C015EA0094912DABF2207A954A84	
11	91a2f29.exe	0C5B5EEE04DE9B791699BB1FEBB55700	PDM:Trojan.Win32.Generic
12	73d1f64.exe	51CCABDBC5D5BD2A4DF0A9D6EB0550FB	HEUR:Trojan.Win32.Cobalt.vho
13	6567131.exe	1956744FDC5F81E05963D6DFF924BD36	
14	C:\Windows\12c4391.exe	1E7475CF5A5AF66A79A4F3F17F875617	HEUR:Trojan.Win32.Cobalt.vho
15	C:\Windows\Temp\rclone.conf	DECBAA664BFBD71B22A31753AFEBDD1A	
Registry & Services			
1	Registry path: HKLM\SYSTEM\ControlSet001\Services\431f9cc		
	Registry value:\\x.x.x.x\ADMIN$\431f9cc.exe		
2	Registry path: HKLM\SYSTEM\ControlSet001\Services\9517238		
	Registry value: \\x.x.x.x\ADMIN$\9517238.exe		
3	Service name: 431f9cc		
	Service file name: \\x.x.x.x\ADMIN$\431f9cc.exe		

No	***Files***	***MD5***	***Remarks***
4	Service name: 522cd6a		
	Service file name: \\x.x.x.x\ADMIN$\522cd6a.exe		
5	Service name: 249f5cb		
	Service file name: \\x.x.x.x\ADMIN$\249f5cb.exe		

Yara Rules Based Signature Detection

```
rule QILIN_ransomware
{
    meta:
        description = "Detects QILIN ransomware IOCs including binaries,
C2 domains, IPs, and email"
    strings:
        // Suspicious Email
        $email = "nopaperplanes@proton.me"

        // Remote IPs
        $ip1 = "180.131.145.73"
        $ip2 = "184.174.96.70"

        // C2 Domains (as strings, any variation with subdomains)
        $domain1 = "misctoolsupdate.com"
        $domain2 = "login.misctoolsupdate.com"
        $domain3 = "sso.misctoolsupdate.com"

        // Malicious Binaries & CobaltStrike (MD5 as hex patterns)
        $md5_1  = { B3 77 FF 70 6F B3 60 06 CD B1 B6 B7 1E 62 B7 E4 }
        $md5_2  = { D2 E1 D5 CE 8B 85 D5 E5 F4 21 06 B2 8C 3F 6E 1E }
        $md5_3  = { F5 1B 82 D0 BA 1B 46 CF 56 C9 BC C8 21 27 FB 45 }
        $md5_4  = { 28 B1 9B 7E 68 9C 33 99 12 79 3F CA 56 27 54 1E }
        $md5_5  = { 01 F8 92 41 2F 9A D5 02 7D 6E 8A 19 EC F5 30 FE }
        $md5_6  = { D2 AB 39 EA 2C 0F CD 17 27 51 F8 4B DA 72 3A 97 }
        $md5_7  = { BE 05 29 FA A5 55 73 6D BF 72 D8 8C B5 0C B3 18 }
        $md5_8  = { 52 E6 66 A3 2D 08 47 B4 16 B6 6A D9 AA 98 BB ED }
        $md5_9  = { D6 30 63 C5 31 68 E4 EA 82 35 EE E6 5E DE A4 E6 }
        $cs_6   = { D1 C4 3F 8D B2 30 BD F1 8C 61 D6 72 44 0E BA 12 }
        $cs_7   = { 71 D6 E5 9E E1 5E 5B 30 D7 FF 1B 56 1E 68 3F 45 }
        $cs_8   = { FF 1C B0 66 59 DA 3E C3 C7 66 22 F7 A4 E9 AB 39 }
        $cs_9   = { AD 39 5D 2D 9C 5F DD 78 A3 55 CB F5 AB 65 FA 62 }
        $cs_10  = { 7D 77 C0 15 EA 00 94 91 2D AB F2 20 7A 95 4A 84 }
        $cs_11  = { 0C 5B 5E EE 04 DE 9B 79 16 99 BB 1F EB B5 57 00 }
        $cs_12  = { 51 CC AB DB C5 D5 BD 2A 4D F0 A9 D6 EB 05 50 FB }
        $cs_13  = { 19 56 74 4F DC 5F 81 E0 59 63 D6 DF F9 24 BD 36 }
        $cs_14  = { 1E 74 75 CF 5A 5A F6 6A 79 A4 F3 F1 7F 87 56 17 }
        $cs_15  = { DE CB AA 66 4B FB D7 1B 22 A3 17 53 AF EB DD 1A }

    condition:
        any of ($email, $ip*, $domain*, $md5*, $cs*)
}
```

Yara Rules Based Behavior Detection

```
rule QilinRansomware {
	meta:
		description = "rule to detect Qilin Ransomware"
		author = "ShadowStackRe.com"
		date = "2023-12-06"
		Rule_Version = "v1"
		malware_type = "ransomware"
		malware_family = "Qilin"
		License = "MIT License, https://opensource.org/license/mit/"
	strings:
		$strMotd = "/etc/motd"
		$strEncryptQuestion = "Are you sure to start encryption"
		$strConfigStart = "--- Configuration start ---"
		$strEsxiUsage = "esxcli"
		$strEncryptRenameFail = "Failed to rename encrypted file to"
		$strStartJob = "Started job..."
		$strBug = "\x1B[%uG 100%%"
	condition:
		all of them
}
```