Description

For SD/MMC cards

Flash memory (common in routers and IoT devices) Another potential way of accessing SD/MMC cards

The device lename for flash memory that supports leops

https://www.cisa.gov/uscert/ncas/alerts/aa22-054a
https://blog.talosintelligence.com/2018/06/vpnlter-update.html?m=1
https://blog.talosintelligence.com/2018/05/VPNFilter.html
https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/
https://media.defense.gov/2022/Jan/25/2002927101/-1/-1/0/CSA_PROTECTING_VSAT_COMMUNICATIONS_012520

community will continue to contribute their findings in the spirit of collaboration that has permeated the threat other binaries and scripts) to these devices in order to conduct their operation.

code on the affected routers, we posit the more plausible hypothesis that the attackers deployed AcidRain (and perhaps We invite the research community to stress test this developmental overlap and contribute their own findings.

and AcidRain taking more of a “one-binary-ts-all” approach to wiping devices. By brute forcing device lenames, the process forking and needless repetition of operations.

More notably, while VPNFilter and AcidRain work in very different ways, both binaries make use of the MEMGETINFO, new

And there are other development quirks, such as the storing of the previous command meant to wipe the devices.

VPNFilter Stage 3 Plugin – ‘dstr’

The reason we bring up the specter of VPNFilter is not because of its superficial similarities to AcidRain but rather plugins, it also included functionality to wipe and brick devices

An Interesting Oddity

exploit had taken place.

When the overwriting method is used instead of the IOCTLs, it copies from a memory region initialized as an array of 4-writes have been committed, the developers run an IOCTLs to erase it: MEMGETINFO, MEMUNLOCK, MEMERASE, and MEMWRITEOOB. In order to make sure that these following this, it attempts to destroy the data in the following storage device files:

Ukrainians – ‘shorthand for “ukr”aine “op”eration, the acronym for the Ukrainian Association of Patriots, or a Russian ethnic slur for

On Tuesday, March 15th, 2022, a suspicious upload caught our attention. A MIPS ELF binary was uploaded to VirusTotal

The AcidRain Wiper

In effect, the preliminary Viasat incident report posits the following requirements:

but not permanently unusable

commands

segment of the KA-SAT network, moved laterally, then used their access to “execute

particular attack goes beyond Ukraine.

conventional warfare. From the beginning of 2022, we have dealt with six different strains of wiper malware targeting

about the role that cyber plays in modern warfare. Some commentators have voiced a

side with their

rendering the modems unable to access the network,

releases a statement

stating that the attack took place in two phases:

Recursively delete files in nonstandard folders

Redundant attempts to reboot the device


<table>
<thead>
<tr>
<th>Name</th>
<th>MD5</th>
<th>SHA256</th>
</tr>
</thead>
<tbody>
<tr>
<td>JUAN ANDRÉS GUERRERO-SAADE</td>
<td>0xffffffff</td>
<td>3C-6F-9A-39-03-C0</td>
</tr>
</tbody>
</table>