AcidRain, a wiper that crippled routers and modems in Europe

April 1, 2022 By Pierluigi Paganini

Researchers spotted a new destructive wiper, tracked as AcidRain, that is likely linked to the recent attack against Viasat.

Security researchers at SentinelLabs have spotted a previously undetected destructive wiper, tracked as AcidRain, that hit routers and modems and that was suspected to be linked to the Viasat KA-SAT attack that took place on February 24th, 2022.

Viasat revealed that a cyberattack hit its KA-SAT network making thousands of modems across Europe unreachable. Company experts noticed that the malicious code issued destructive commands to overwrite key data in flash memory on the modems, rendering the modems unable to access the network, but not permanently unusable.

describe the attack. "Ultimately, tens of thousands of modems that were previously online and active dropped off the network, and these modems were not observed attempting to re-enter the network. The attack impacted a majority of the previously active modems within Ukraine, and a substantial number of additional modems in other parts of Europe."

5,800 Enercon wind turbines in Germany were unreachable due to the spillover from this attack.

According to the experts, AcidRain is an ELF MIPS malware specifically designed to wipe modems and routers.

"The preliminary Viasat incident report posits the following requirements:

1. *Could be pushed via the KA-SAT management segment onto modems en masse*
2. *Would overwrite key data in the modem's flash memory*
3. *Render the devices unusable, in need of a factory reset or replacement but not permanently unusable." reads the analysis published by SentinelOne.*

"The threat actor used the KA-SAT management mechanism in a supply-chain attack to push a wiper designed for modems and routers."

SentinelLabs assessed with medium-confidence that there are developmental similarities between AcidRain and the Russia-linked VPNFilter stage 3 destructive plugin.

Location	String Value	String Representati...	Data Type
.shstrtab::00000001	.shstrtab	".shstrtab"	ds
.shstrtab::0000000b	.reginfo	".reginfo"	ds
.shstrtab::00000014	.init	".init"	ds
.shstrtab::0000001a	.text	".text"	ds
.shstrtab::00000020	.fini	".fini"	ds
.shstrtab::00000026	.rodata	".rodata"	ds
.shstrtab::0000002e	.eh_frame	".eh_frame"	ds
.shstrtab::00000038	.ctors	".ctors"	ds
.shstrtab::0000003f	.dtors	".dtors"	ds
.shstrtab::00000046	.jcr	".jcr"	ds
.shstrtab::0000004b	.data	".data"	ds
.shstrtab::00000051	.got	".got"	ds
.shstrtab::00000056	.sbss	".sbss"	ds
.shstrtab::0000005c	.bss	".bss"	ds
.shstrtab::00000061	.mdebug.abi32	".mdebug.abi32"	ds
.shstrtab::0000006f	.pdr	".pdr"	ds

Location	String Value	String Representation	Data
.shstrtab::00000001	.shstrtab	".shstrtab"	ds
.shstrtab::0000000b	.reginfo	".reginfo"	ds
.shstrtab::00000014	.init	".init"	ds
.shstrtab::0000001a	.text	".text"	ds
.shstrtab::00000020	.fini	".fini"	ds
.shstrtab::00000026	.rodata	".rodata"	ds
.shstrtab::0000002e	.eh_frame	".eh_frame"	ds
.shstrtab::00000038	.ctors	".ctors"	ds
.shstrtab::0000003f	.dtors	".dtors"	ds
.shstrtab::00000046	.jcr	".jcr"	ds
.shstrtab::0000004b	.data	".data"	ds
.shstrtab::00000051	.got	".got"	ds
.shstrtab::00000056	.sbss	".sbss"	ds
.shstrtab::0000005c	.bss	".bss"	ds
.shstrtab::00000061	.mdebug.abi32	".mdebug.abi32"	ds
.shstrtab::0000006f	.pdr	".pdr"	ds

AcidRain is the 7th wiper malware used by threat actors since the beginning of the Russian invasion of Ukraine. A sample of the AcidRain Wiper was uploaded to VirusTotal from Italy with the name 'ukrop.'

Experts believe that the wiper is not complex and leverage bruteforce attacks to compromise the devices, the malicious code is able to wipe the device and storage device files.

"The binary performs an in-depth wipe of the filesystem and various known storage device files. If the code is running as root, AcidRain performs an initial recursive overwrite and delete of non-standard files in the filesystem." concludes the report. "Despite Viasat's statement claiming that there was no

Pierluigi Paganini

(**SecurityAffairs – hacking, AcidRain** wiper)

Pierluigi Paganini

Pierluigi Paganini is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group and Cyber G7 Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE

Zyxel fixes a critical bug in its business firewall and VPN devices

NEXT ARTICLE

Anonymous targets oligarchs' Russian businesses: Marathon Group hacked

YOU MIGHT ALSO LIKE

Google announced the completion of the acquisition of Mandiant for $5.4 billion