The Good

This week, the United States and the European Union confirmed Russian involvement in a series of destructive cyber attacks in February 2022 against Ukrainian organizations and infrastructure.

These attacks targeted commercial satellite communication networks run by Viasat, a US-based communication firm. The actors responsible deployed the AcidRain wiper malware to destroy thousands of satellite modems, and disrupted the operation of over 5,800 wind turbines.

In a statement, US Secretary of State Antony Blinken condemned Russia's cyber attacks against Ukraine, outlining the "website defacements, distributed denial-of-service (DDoS) attacks, and cyber attacks to delete data from computers belonging to government and private entities" in the months leading up to Russia's invasion.

Blinken then offered more detail into the United States assessment of the AcidRain campaign, which he said "disabled very small aperture terminals in Ukraine and across Europe. This includes tens of thousands of terminals outside of Ukraine that, among other things, support wind turbines and provide Internet services to private citizens."

The State Department's assessment, alongside Viasat's investigation results, reflects SentinelOne's analysis of the AcidRain wiper. During this attack, a destructive MIPS ELF binary wiped out filesystems, flash memories, and SD/MMC cards on vulnerable modems.

In response, the United States government is rolling out new measures to help Ukraine with detection, response and recovery. The government is also supporting Ukraine's communication capabilities by supplying satellite phones and data terminals to support Ukraine's government and infrastructure.

The Bad

The US Cybersecurity and Infrastructure Security Agency's (CISA) latest update to its Known Exploited Vulnerabilities Catalog recommends that users of F5 Networks' BIG-IP iControl REST service patch their systems to address a critical vulnerability.

The bug (tracked as CVE-2022-1388 with a CVSS score of 9.8) allows threat actors to bypass authentication and access vulnerable devices to execute remote code, make configuration changes, move laterally within a compromised network or exfiltrate data.

On May 4, 2022, F5 released initial patches for the vulnerability alongside an advisory disclosing technical details surrounding the flaw to users. While the company has also released indicators of compromise (IOCs) in the past week, its updated advisory still warns that skilled attackers can mask their presence in a system when they gain access.

Despite F5's attempts to mitigate the fallout, security experts have observed attackers exploiting the critical flaw in the wild this week. Unfortunately, the SANS Internet Storm Center has also discovered attackers leveraging the bug to wipe servers and make them unusable.

Researchers have also expressed concern about the risk that more attackers will attempt to exploit the vulnerability because it requires little technical skill.

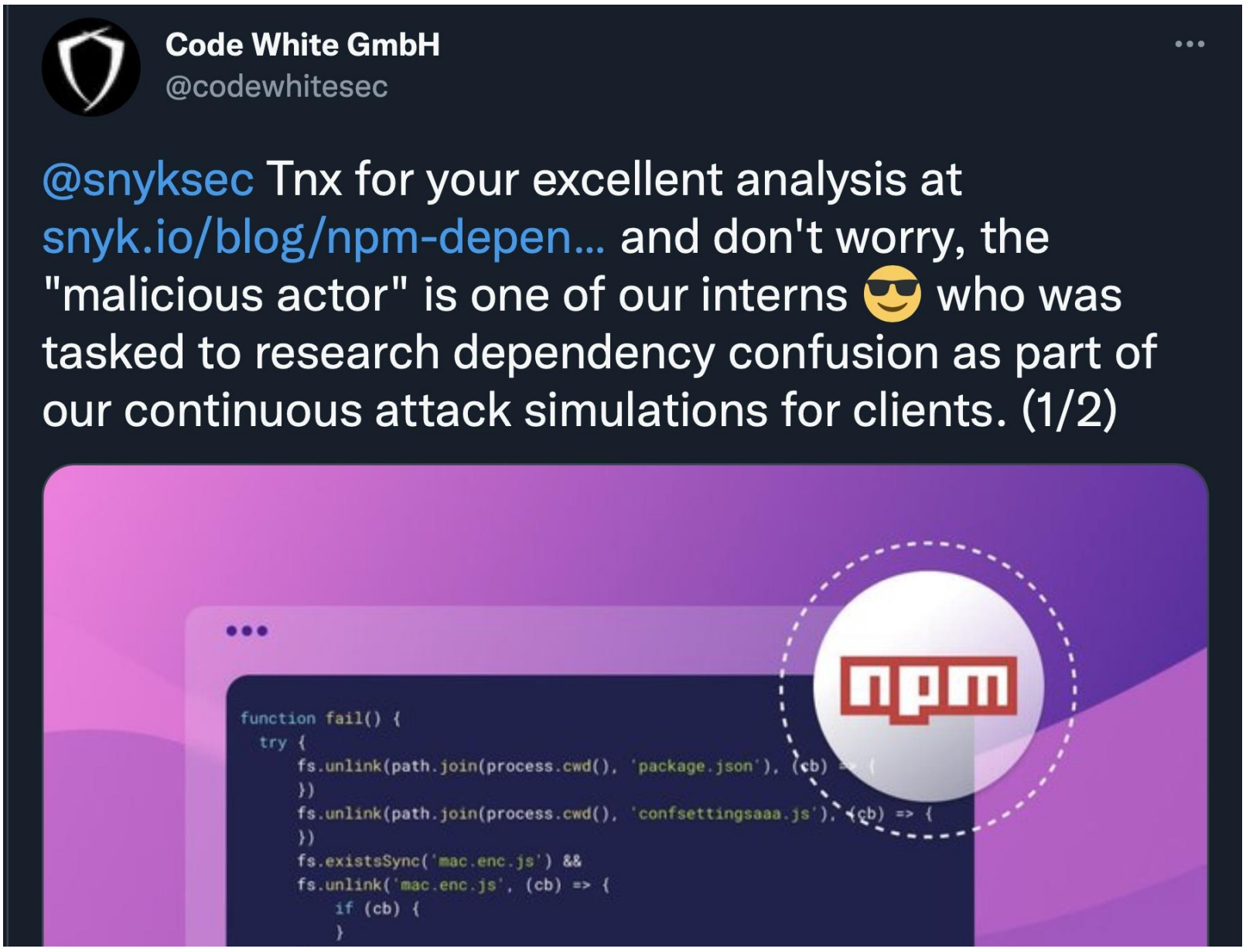
Due to the growing risk surrounding this critical vulnerability, CISA and other federal agencies recommend that all impacted users patch their systems as soon as possible.

The Ugly

Over the past few weeks, security researchers have been actively investigating four backdoors discovered within open source code. Analysis showed the actor behind the backdoors was targeting four German companies and using a new form of supply chain attack called "dependency confusion".

As the name suggests, dependency confusion relies on tricking targets into downloading dependent, third-party code from the wrong location.

But in a surprising turn of events, the "threat actor" behind these particular backdoors came forward to reveal themselves. Code White, a penetration testing firm, announced that they were "trying to mimic realistic threat actors for dedicated clients as part of [their] Security Intelligence Service," and that the "malicious actor" in question was an intern for the firm. Code White's CEO confirmed that the affected companies had requested penetration testing exercises and that the firm had assembled the code dependencies to simulate real threats.



The public nature of the attacks meant others aside from Code White's clients were unwittingly pulled into the exercise and arguably wasted valuable research time [1, 2] analysing what appeared to be real threats delivering malware via an open source public repository.

On the other hand, perhaps this unusual incident may help raise awareness of dependency confusion attacks among other organizations, too. Security experts have noted that although the Code White dependency confusion exercises don't count as a sign that these types of attacks are on the rise, it's possible that attackers will begin leveraging this attack vector in the future.