The Good

In the face of a cyber attack launched by the Hive ransomware group, the Bank of Zambia offered a particularly creative response to their attackers' ransom note.

On May 13th, the Bank of Zambia released a public statement informing the public that they had been targeted by cyber criminals, and that the attack had caused "partial disruptions to some of its Information Technology (IT) applications on Monday, 9th May 2022."

According to a recent report, the Hive ransomware group purportedly encrypted the Bank of Zambia's Network Attached Storage (NAS) device. In response, representatives of the bank refused to pay the demanded ransom and chose to mock the hackers in their initial response.

The bank then linked a picture of male genitalia and told the attackers to "suck [it]" and "learn to monetize" because locking bank networks would be ineffective.

Although security experts assumed that unrelated parties had hijacked the negotiation chat, Greg Nsofu, Technical Director at the Bank of Zambia, tacitly confirmed that this was not the case.

Once the bank confirmed that its core systems were protected from the attack, Nsofu stated that the bank's response "pretty much told them where to get off."

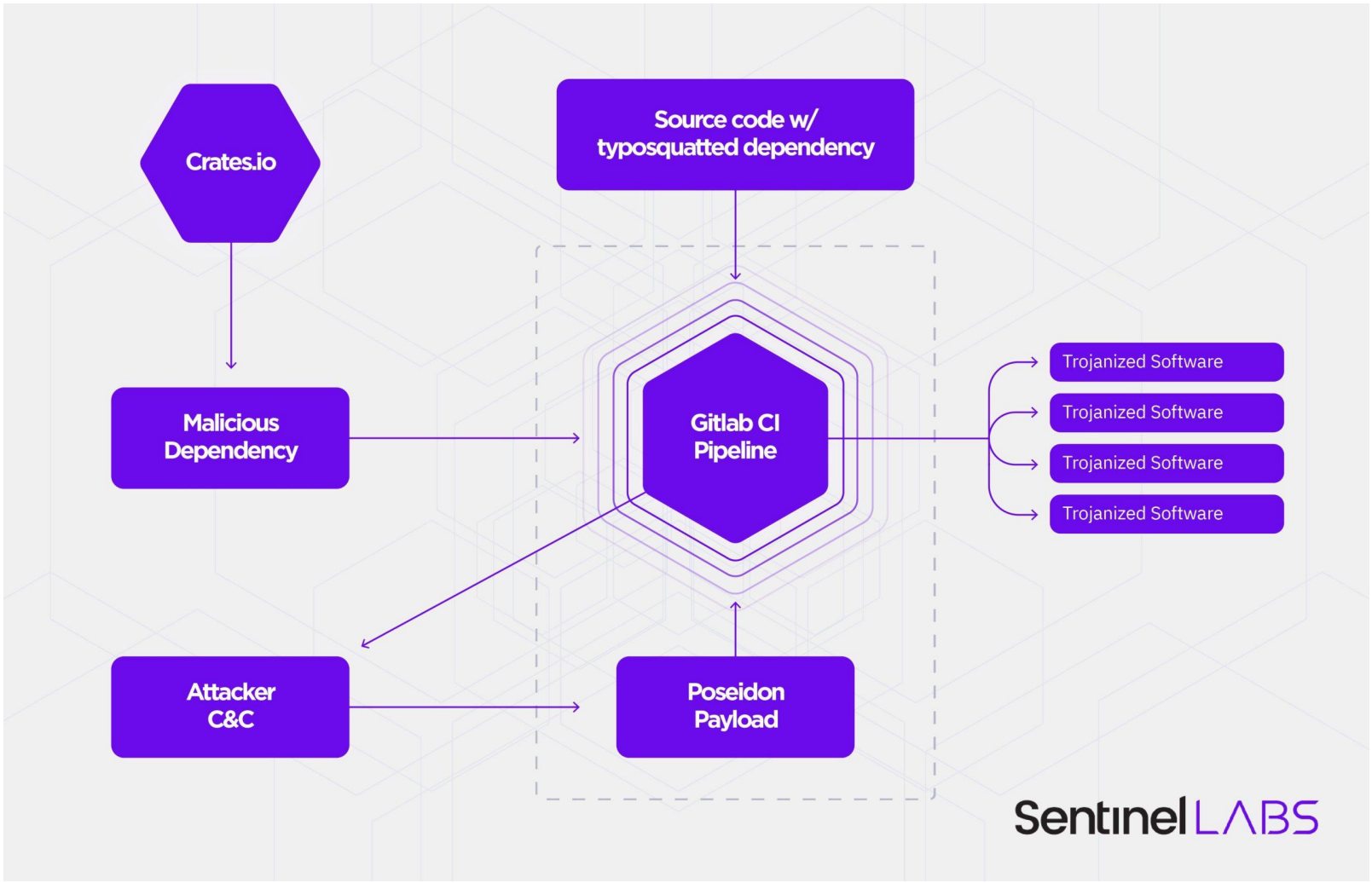
Although this was an unorthodox response to threat actors, the Bank of Zambia's proactive steps to protect their core systems and clear refusal to pay the ransom are exemplary of how organizations should prepare and respond to ransomware attacks.

The Bad

On May 19th, 2022, SentinelLabs shared their initial findings on a supply-chain attack against the Rust programming language development community, referred to as CrateDepression.

In an advisory published on May 10th, the Rust Security Response Working Group disclosed the discovery and removal of a malicious compilation unit from the crates.io community repository.

Security experts found that the threat actors attempted to impersonate a trusted Rust developer and uploaded malware to the Rust dependency community repository. The attacker(s) named their malicious crate "rustdecimal" in an attempt to typosquat and fool Rust developers looking to use the well-known rust_decimal crate.



Once the malicious crate infects a machine, the machine is scanned for the "GITLAB_CI" environment variable to identify GitLab Continuous Integration (CI) pipelines for software development. Infected CI pipelines are used to deliver a second-stage payload. The SentinelLabs team has identified these payloads as Go binaries built on the Mythic agent "Poseidon," a red-teaming framework.

Although the responsible threat actors' intent is currently unknown, the nature of their targets indicate that this attack could enable subsequent, larger scale supply-chain attacks relative to the development pipelines infected.

The Rust security team's advisory recommends that organizations and projects running GitLab CI pipelines check whether they depended on the rustdecimal crate, starting from March 25th, 2022. If a dependency on that crate is detected, the CI environment may be compromised. The advisory also recommends regular dependency audits and exclusively using crates from trusted authors.

The SentinelLabs team has also assembled several Indicators of Compromise (IOCs) to assist security teams with proactive threat hunting, detection and response, which you can access here.

The Ugly

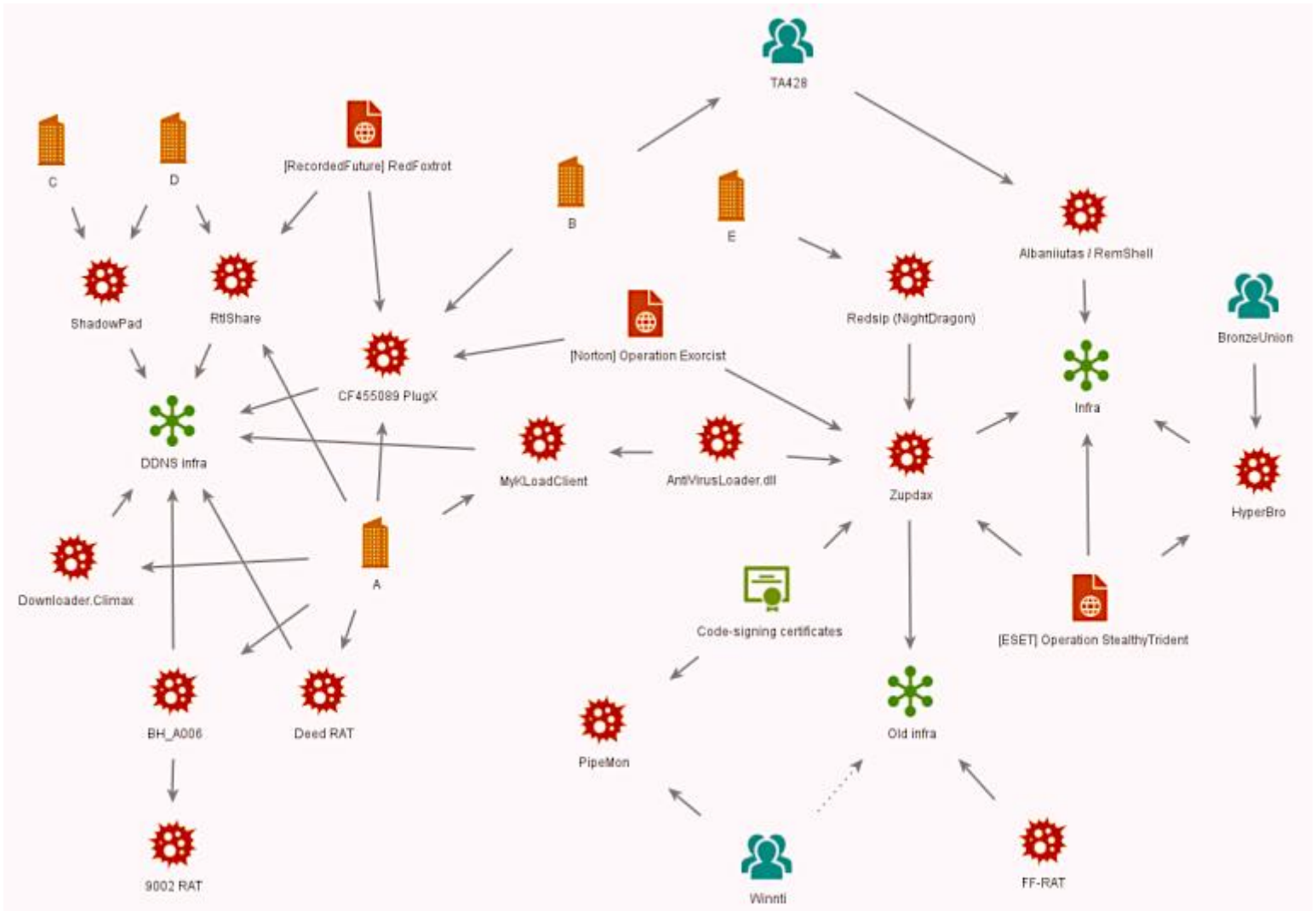
In the latest news surrounding international cyber attacks, an emerging Chinese threat group (dubbed "Space Pirates" by Russian threat analysts) is targeting Russian aerospace firms with phishing emails.

Analysts have determined that phishing emails sent to Russian, Mongolian and Georgian government-affiliated and private organizations in the aerospace, electric power and IT industries were designed to install custom malware and exfiltrate sensitive data from infected environments.

The Space Pirates were first observed while security professionals were responding to an incident in the summer of 2021, but analysts theorize that the group may have been active since at least 2019. A recent report found that the Space Pirates' malware and infrastructure had been sighted in similar attacks, including two successful campaigns against state-sponsored Russian organizations.

During these attacks, the group was able to maintain access to servers and networks for extended periods of time, ranging from ten months up to over a year, stealing confidential documents, employee data and other critical information.

According to the findings, the cluster of activity attributed to the Space Pirates APT is just the latest in a rising trend of escalating attacks from Chinese threat actors against Russian entities. The threat group deploys signature Chinese malware such as ShadowPad and PlugX among a complex range of modular malware tools, custom loaders, and modified backdoors.



Chinese threat actors are also known to leverage tool exchanges and share tools to make it harder to identify specific threat groups, posing a difficult and taxing challenge for security professionals looking to identify threats and protect their systems. For organizations without modern defenses, these APTs and their malware continue to pose a serious risk.