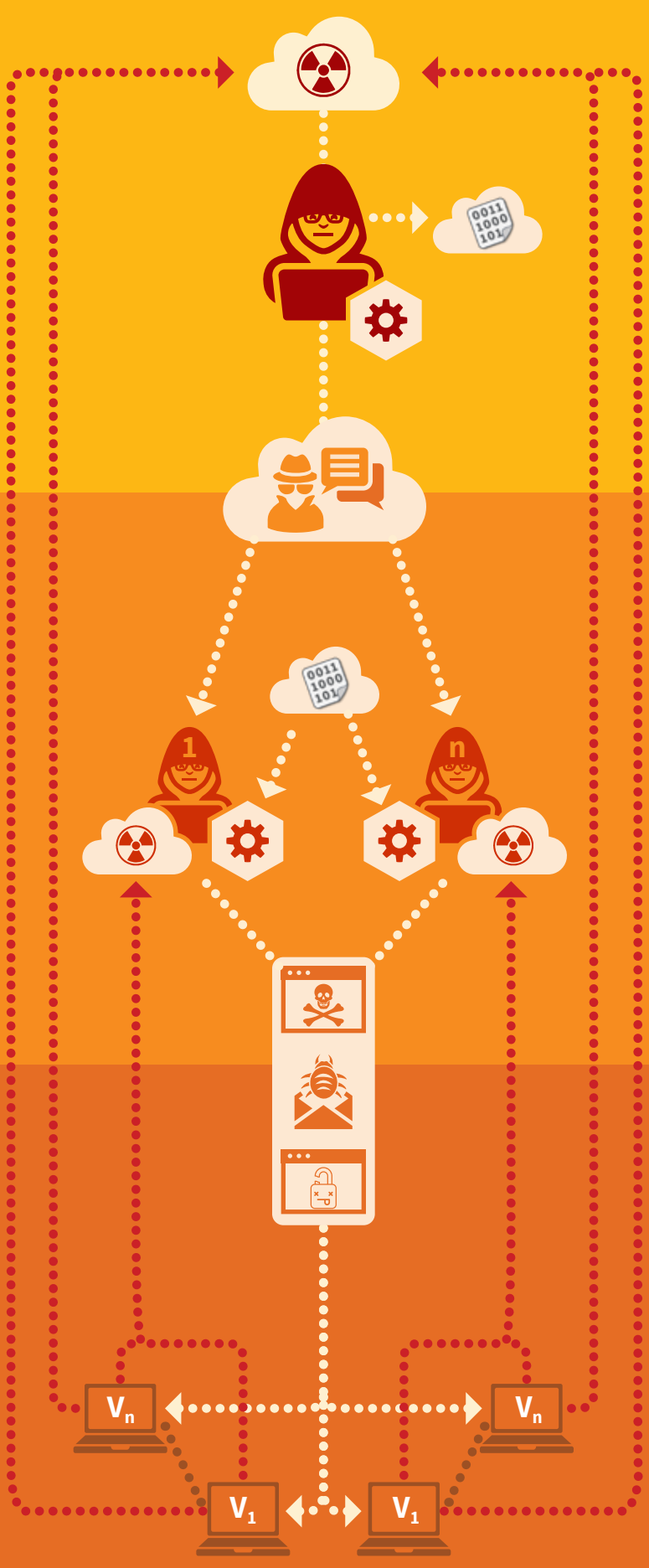
Cobian RAT – A Backdoored RAT

A free RAT builder with a message: *you get what you pay for.*

The author of the Cobian remote access Trojan (RAT) builder advertises the kit for free on underground forums. But unbeknownst to the second-level malware operators who use it, the kit contains a hidden backdoor that is controlled by the original author.

1

The second-level operators use the builder kit to generate RAT payloads, which they distribute via spam emails and/or compromised websites to build and control their own botnets. Meanwhile, the backdoored builder kit silently pulls C&C information from the original author-controlled pastebin URL.



2

User systems compromised by the malicious payload initially communicate with the C&C server configured by the second-level operator, but they get subsequent instructions to communicate with the original author's C&C. The original author is able to take full control of compromised systems, and, if desired, cut off all communications to the second-level malware operator.

3

> "The Cobian RAT appears to be yet another RAT spawned from the leaked njRAT source code. **It's ironic watching these second-level operators** use the kit to propagate malware in order to steal from their victims, when, in fact, **they themselves are being duped** into doing the dirty work for the original author."
>
> *– **Deepen Desai,** Senior Director, Security Research*

ThreatLabZ is the research division of Zscaler, builder and operator of a purpose-built, globally distributed security cloud, which safeguards thousands of organizations against malware, data loss, and other threats. **zscaler.com**