

Forum:[Hack Forums](#)

Thread: [\[Theory\] The IDE Crasher's Guide To A Leaky Bucket Lexicon Bomb \[Theory\]](#)

KodaKing - May 12, 2018, 7:46 am

The IDE Crasher's Guide To A Leaky Bucket Lexicon Bomb

Written by °KodaKing°

With modern systems and devices utilizing regularly accessible push commands, the ability to over code emission signals, and a wonderful allotment of code option we find a standing opponent. The nature of the hacker is routed in the ability to provide a new approach but our community wishes for script kiddies and not for our real script.

When noted that all antivirus, anti-malware, and screening applications use preconfigured code samples, we note a demand for FUD crypters.

No more trivial child's play, no more ignorance: where is my steak, my creme brulee, my 250\$ bottle of Cabernet - I'm tired of this shit and bread.

Take the Rosetta stone - tons of languages set to be translated with similar text.

With a crafted packet using various languages all as code word reference in different encryptions, all with no direct grammar or syntax you find a packet of (at view) meaningless info.

Now make nine of them - use c#, use angular, use java, use perl, Ruby on rails, and lisp... Use nfc encoded RF short code, assembly, binary...

Package a randomized list of your malicious keyterms and no applicable trace route to the payoff.

New packets - your translation.

C# has to be compiled, angular a bit easier. Java can run soft others need library patching, but with these components prepared in the prior, make a design for your translator on paper. Look at what compiler options need to be grafted, what libraries to be accessed. Write these down.

Timeline what can be done in order which won't flag the av, and what Mal code you can't translate in the first two steps, figure out a silent seizure to exploit the ignore or whitelist options and acting as a fake quarantined file you can silently build the rest.

Write out your connection files to build the similar components by translation on DL completion. Set up two to three files to do this quietly from the False Quarantine.

Let your last packet of meaningless index connectors finalize the source and activate the payload. With push commands written to flawlessly resemble a regular source whether it be from a careful crafted app, a run time RAT, or even a poisoned wifi, gsm, or push signal (yes there are push services you can access) then you can load the victim machine without notice.

Zero Day Everything.

Happy Hacking.

-°Koda°-