New NKAbuse malware abuses NKN blockchain for stealthy comms

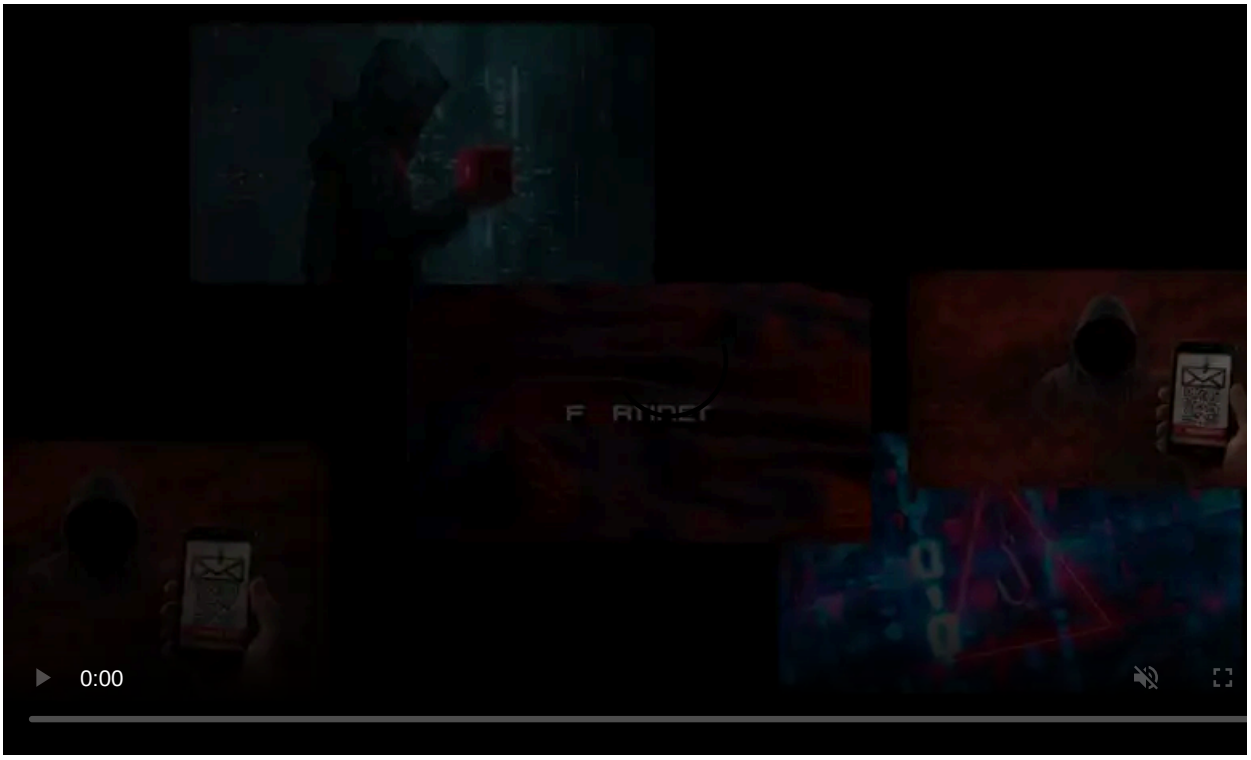
By Bill Toulas

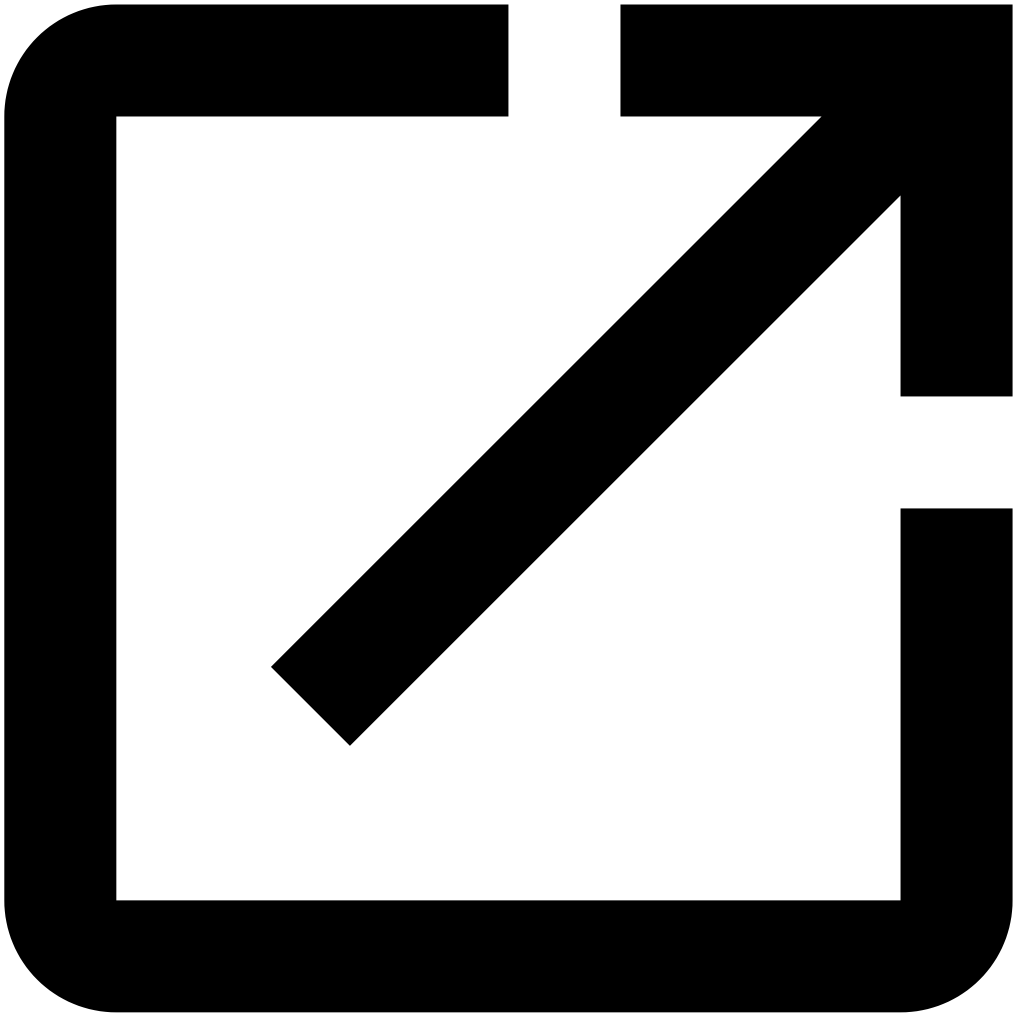
Published: 2023-12-14 · Archived: 2026-04-05 21:50:04 UTC

A new Go-based multi-platform malware identified as 'NKAbuse' is the first malware abusing NKN (New Kind of Network) technology for data exchange, making it a stealthy threat.

NKN is a relatively new decentralized peer-to-peer network protocol leveraging blockchain technology to manage resources and maintain a secure and transparent model for network operations.

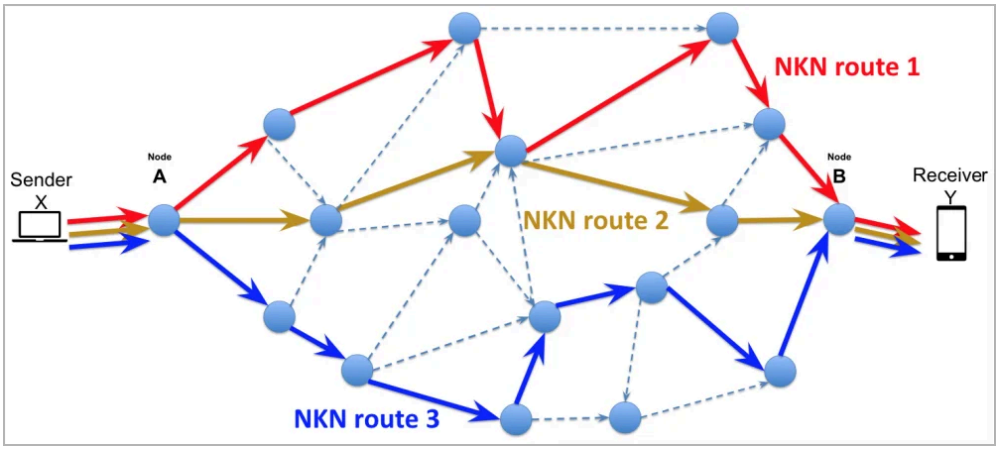
One of the goals of NKN is to optimize data transmission speed and latency across the network, which is achievable by calculating efficient data packet travel paths.


0:00



Individuals can participate in the NKN network by running nodes, similar to the Tor network, and currently, there are approximately 60,710 nodes in it.

This relatively large number of nodes contributes to robustness, decentralization, and ability to handle significantly high volumes of data.



Moving data through NKN *(Kaspersky)*

NKAbuse details

Kaspersky reports the discovery of a novel malware named NKAbuse, which primarily targets Linux desktops in Mexico, Colombia, and Vietnam.

One NKAbuse infection spotted by Kaspersky involves the exploitation of an old Apache Struts flaw (CVE-2017-5638) to attack a financial company.

Although most attacks target Linux computers, the malware can compromise IoTs and supports MIPS, ARM, and 386 architectures.

NKAbuse abuses NKN to launch DDoS (distributed denial of service) attacks that are hard to trace back to a specific infrastructure and unlikely to be flagged due to originating from a novel protocol not actively monitored by most security tools.

"This threat (ab)uses the NKN public blockchain protocol to carry out a large set of flooding attacks and act as a backdoor inside Linux systems." explains Kaspersky

Specifically, the malware client communicates with the bot master through NKN to send and receive data. At the same time, its ability to keep multiple concurrent channels alive gives resilience to its communication line.

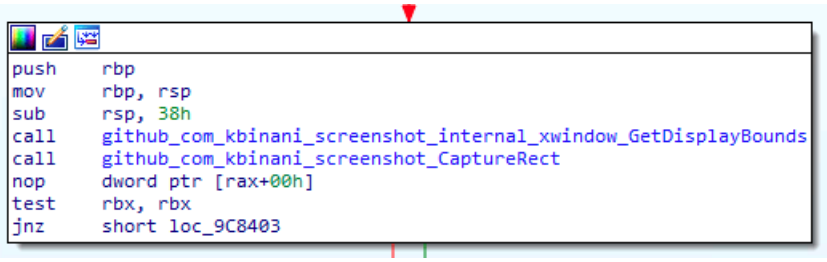
The payload commands sent by the C2 include HTTP, TCP, UDP, PING, ICMP, and SSL flood attacks aimed at a specified target.

Command	Attack
Default/0	http_flood_HTTPGetFloodPayload
1	http_flood_HTTPPostFloodPayload
2	tcp_flood_TCPFloodPayload
3	udp_flood_UDPFloodPayload
4	ping_flood_PINGFloodPayload
5	tcp_syn_flood_TCPSynFloodPayload
6	ssl_flood_SSLFloodPayload
7	http_slowloris_HTTPSlowlorisPayload
8	http_slow_body_HTTPSlowBodyPayload
9	http_slow_read_HTTPSlowReadPayload
10	icmp_flood_ICMPFloodPayload
11	dns_nxdomain_DNSNXDOMAINPayload

DDoS attack commands *(Kaspersky)*

"All these payloads historically have been used by botnets, so, when combined with the NKN as the communication protocol, the malware can asynchronously wait for the master to launch a combined attack," Kaspersky says.

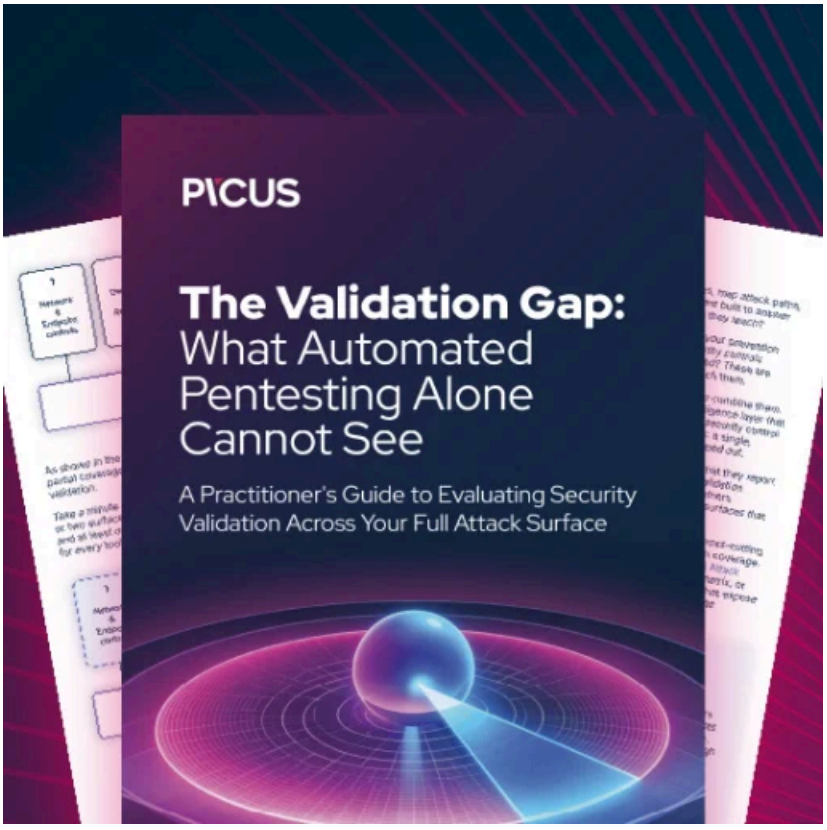
In addition to the DDoS capabilities, NKAbuse also acts as a remote access trojan (RAT) on compromised systems, allowing its operators to perform command execution, data exfiltration, and snap screenshots.



Screenshot functionality *(Kaspersky)*

This plethora of capabilities that make NKAbuse highly versatile and adaptive isn't typical in the DDoS botnet space.

Additionally, using blockchain technology that guarantees availability and obfuscates the source of the attacks makes defending against this threat very challenging.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
