Pagina 7 - New Supply Chain Malware Operation Hits npm and PyPI Ecosystems, Targeting Millions Globally

Classificações de Malware:

- trojan (Trojan)
- trojanized (Trojan)
- infection (Virus)
- backdoor (Backdoor)
- rat (Backdoor)
- rootkit (Rootkit)
- stealth (Rootkit)
- ransomware (Ransomware)
- exploit (Exploit)
- virus (Virus)
- adware (Adware)
- ads (Adware)

Cybersecurity researchers haveflaggeda supply chain attack targeting over a dozen packages associated with Glu
eStack to deliver malware.The malware, introduced via a change to "lib/commonjs/index.js," allows an attacker
to run shell commands, take screenshots, and upload files to infected machines, Aikido Security told The Hacke
r News, stating these packages collectively account for nearly 1 million weekly downloads.The unauthorized acc
ess could then be used to perform various follow-on actions like mining cryptocurrency, stealing sensitive inf
ormation, and even shutting down services. Aikido said the first package compromise was detected on June 6, 20
25, at 9:33 p.m. GMT.The list of the impacted packages and the affected versions is below -Furthermore, the ma
licious code injected into the packages issimilarto the remote access trojan that was delivered following the
compromise of another npm package "rand-user-agent" last month, indicating that the same threat actors could b
e behind the activity.The trojan is an updated version that supports two new commands to harvest system inform
ation ("ss_info") and the public IP address of the host ("ss_ip").The project maintainers have

sincerevoked th
e access tokenand marked the impacted versions as deprecated. Users who may have downloaded the malicious vers
ions are recommended to roll back to a safe version to mitigate any potential threats."The potential impact is
massive in scale, and the malware's persistence mechanism is particularly concerning attackers maintain acces
s to infected machines even after maintainers update the packages," the company said in a statement.However, i
n an incident report published on June 9, 2025, the project maintainers acknowledged that a public access toke
n associated with one of their contributors was compromised, thereby allowing threat actors to publish tampere
d versions of react-native-aria packages along with a @gluestack-ui/utils package to npm."The compromised pack
age was published by a compromised account of an authorized maintainer," Suraj Ahmed Choudhurysaid. "React Nat
ive ARIA is a frontend-only library. It does not execute any code in CLI or scripts post-install, meaning the
likelihood of the malicious code executing on user systems is extremely low to none. Based on our current unde
rstanding and usage patterns, no system-level compromises are expected."The maintainers also said they have al
so revoked GitHub repository access for all non-essential contributors, and enabled two-factor authentication
(2FA) for publishing and GitHub access.The development comes as Socket discovered two rogue npm packages expre
ss-api-sync and system-health-sync-api that masquerade as legitimate utilities but implant wipers that can del
ete entire application directories.Published by the account "botsailer" (email: anupm019@gmail[.]com), the pac
kages were downloaded 112 and 861 times, respectively, before being taken down.The first of the two packages,
express-api-sync, claims to be an Express API to sync data between two databases. However, once installed and
added by an unsuspecting developer to their application, it triggers the execution of malicious code upon rece
iving an HTTP request with a hard-coded key "DEFAULT_123."Upon receipt of the key, it

executes the Unix comman
d "rm -rf *" to recursively delete all files from the current directory and below, including source code, conf
iguration files, assets, and local databases.The other package is a lot more sophisticated, acting both as an
information stealer and a wiper, while also modifying its deletion commands based on whether the operating sys
tem is Windows ("rd /s /q .") or Linux ("rm -rf *")."Where express-api-sync is a blunt instrument, system-heal
th-sync-api is a Swiss Army knife of destruction with built-in intelligence gathering," security researcher Ku
sh Pandyasaid.A notable aspect of the npm package is that it uses email as a covert communication channel, con
necting to the attacker-controlled mailbox via hard-coded SMTP credentials. The password is obfuscated using B
ase64-encoding, whereas the username points to an email address with a domain that's associated with a real es
tate agency based in India ("auth@corehomes[.]in")."Every significant event triggers an email to anupm019@gmai
l[.]com," Socket said. "The email includes the full backend URL, potentially exposing internal infrastructure
details, development environments, or staging servers that shouldn't be publicly known."The use of SMTP for da
ta exfiltration is sneaky as most firewalls do not block outbound email traffic, and allows malicious traffic
to blend in with legitimate application emails.Furthermore, the package resisters endpoints at "/_/system/heal
th" and "/_/sys/maintenance" to unleash the platform-specific destruction commands, with the latter acting as
a fallback mechanism in case the main backdoor is detected and blocked."Attackers first verify the backdoor vi
a GET /_/system/health which returns the server's hostname and status," Pandya explained. "They can test with
dry-run mode if configured, then execute destruction using POST /_/system/health or the backup POST /_/sys/mai
ntenance endpoint with the key "HelloWorld."The discovery of the two new npm packages shows that threat actors
are beginning to branch out beyond using bogus libraries for information and cryptocurrency

theft to focus on
system sabotage -- something of an unusual development as they offer no financial benefits.It also comes as t
he software supply chain security firm discovered a new Python-based credential harvester imad213 on the Pytho
n Package Index (PyPI) repository that claims to be an Instagram growth tool. According to statistics publishe
d on pepy.tech, the package has been downloaded 3,242 times."The malware uses Base64-encoding to hide its true
nature and implements a remote kill switch through a Netlify-hosted control file," Pandyasaid. "When executed
, it prompts users for Instagram credentials, and broadcasts them to ten different third-party bot services wh
ile pretending to boost follower counts."The Python library has been uploaded by a user namedim_ad__213(aka IM
AD-213), who joined the registry on March 21, 2025, and has uploaded three other packages that can harvest Fac
ebook, Gmail, Twitter, and VK credentials (taya, a-b27) or leverage Apache Bench to target streaming platforms
and APIs with distributed denial-of-service (DDoS) attacks (poppo213).The list of packages, which are still a
vailable for download from PyPI, is below -In a GitHub README.md document published by IMAD-213 about two days
before "imad213" was uploaded to PyPI, the threat actorclaimsthat the library is mainly for "educational and
research purposes" and notes that they are not responsible for any misuse.The GitHub description also includes
a "deceptive safety tip," urging users to utilize a fake or temporary Instagram account to avoid running into
any issues with their main account."This creates false security, users think they're being cautious while sti
ll handing over valid credentials to the attacker," Pandya said.Once launched, the malware connects to an exte
rnal server and reads a text file ("pass.txt") and proceeds further with the execution only if the file conten
t matches the string "imad213." The kill switch can serve multiple purposes, allowing the threat actor to dete
rmine who gets access to run the library or turn off every downloaded copy by simply

changing the context of t
he control file.In the next step, the library prompts the user to enter their Instagram credentials, which are
then saved locally in a file named "credentials.txt" and broadcast to ten different dubious bot service websi
tes, some of which link to a network of Turkish Instagram growth tools likely operated by the same entity. The
domains were registered in June 2021."The emergence of this credential harvester reveals concerning trends in
social media-targeted malware," Socket said. "With ten different bot services receiving credentials, we're se
eing the early stages of credential laundering where stolen logins are distributed across multiple services to
obscure their origin."Discover real-time defense tactics to detect and block deepfakes, fake domains, and mul
ti-channel scams before they cause damage.We'll unpack how leading teams are using AI, privacy-first design, a
nd seamless logins to earn user trust and stay ahead in 2025.Get the latest news, expert insights, exclusive r
esources, and strategies from industry leaders all for free.

Link: https://thehackernews.com/2025/02/chinese-linked-attackers-exploit-check.html