Pagina 3 - Iran Slows Internet to Prevent Cyber Attacks Amid Escalating Regional Conflict

Classificações de Malware:

- crypto (Ransomware)
- ransomware (Ransomware)
- exploit (Exploit)
- cve (Exploit)
- trojan (Trojan)
- dropper (Trojan)
- backdoor (Backdoor)
- rootkit (Rootkit)
- rat (Backdoor)
- virus (Virus)

Iran has throttled internet access in the country in a purported attempt to hamper Israel's ability to conduct
covert cyber operations, days after the latter launched an unprecedented attack on the country, escalating ge
opolitical tensions in the region.Fatemeh Mohajerani, the spokesperson of the Iranian Government, and the Iran
ian Cyber Police, FATA,saidtheinternet slowdownwasdesignedto maintain internet stability and that the move is
"temporary, targeted, and controlled, to ward off cyber attacks." Datasharedby NetBlocks shows a "significant
reduction in internet traffic" around 5:30 p.m. local time.The development comes amid deepening conflict, with
Israel and Iran trading missile attacks since Friday. These attacks have spilled over into cyberspace, as sec
urity experts warned of retaliatory cyber operations by Iranian state actors and hacktivist groups.The digital
warfare unfolding behind the scenes goes two ways. Earlier this week, a pro-Israeli group known asPredatory S
parrowclaimed responsibility for a cyber attack on Iran's Bank Sepah,crippling accessto its website and ATMs."
'Bank Sepah' was an institution thatcircumvented international sanctionsand used the people of Iran's money to
finance the regime's terrorist proxies, its ballistic missile program, and its military nuclear

program," the
groupsaidin a public statement posted on X.Predatory Sparrow also said it sabotaged the bank's infrastructure
with help from "brave Iranians," adding "this is what happens to institutions dedicated to maintaining the di
ctator's terrorist fantasies." Israel has a storied history ofsophisticatedcyber operations, most notably theS
tuxnetattack targeting Iran's nuclear program.Tel Aviv-based cybersecurity firm Radwaresaidit has observed hei
ghtened activity from threat actors affiliated with Iran across public and private Telegram channels.Some of t
he groups, including Mysterious Team Bangladesh and Arabian Ghost, have warned neighboring countries Jordan an
d Saudi Arabia against supporting Israel and claimed to have shut down Israeli radio stations.Furthermore, the
Iranian government has urged citizens to delete WhatsApp, one of the country's most popular messaging platfor
ms, stating without giving any evidence that the Meta-owned app has been weaponized by Israel to spy on its us
ers.WhatsApp has denied the allegations. In astatementto the Associated Press, the company said it does not tr
ack users nor does it provide "bulk information to any government."The cyber conflict also follows an announce
ment from the U.S. Department of State that they were seeking information on Iranian hackers who they accused
of targeting critical infrastructure in the U.S., Israel, and other countries using theIOCONTROL(aka OrpaCrab)
malware to breach Industrial Control Systems (ICS)."Cyber Av3ngers, which is associated with the online perso
na Mr. Soul, has launched a series of malicious cyber activities against U.S. critical infrastructure on behal
f of Iran's Islamic Revolutionary Guard Corps Cyber-Electronic Command (IRGC-CEC)," the department's Rewards f
or Justice (RFJ) programsaid."Cyber Av3ngers actors have utilized malware known as IOCONTROL to target ICS/SCA
DA devices used by critical infrastructure sectors in the United States and worldwide."On June 18, Predatory S
parrowsaidit was behind a cyber attack on Iranian cryptocurrency exchange Nobitex. The

hacktivist collective a
lso said they would publish the platform's source code and data from its internal network within 24 hours."The
Nobitex exchange is at the heart of the regime's efforts to finance terror around the world," the group said.
"This exchange is the regime's most popular tool for circumventing international sanctions."In a security ale
rt, Nobitexsaidit suspended all access after it detected "signs of unauthorized access to a portion of our rep
orting infrastructure and hot wallet." It further reassured users that all of their assets are secure and that
it would compensate for all damages.According to blockchain investigator ZachXBT, around $81.7 million worth
of digital assets werestolenfrom the exchange across Tron, EVM and BTC chains. "The attacker used the vanity a
ddress TKFuckiRGCTerroristsNoBiTEXy2r7mNX," ZachXBTsaidin a post on Telegram.Blockchain analysis firm Elliptic
said the hackers "burned" the stolen funds by sending them to inaccessible wallets, effectively pulling the a
ssets out of circulation. It also noted that it identified the use of Nobitex by sanctioned operatives from th
e Iranian Islamic Revolutionary Guard Corps (IRGC)."The hack also does not appear to be financially motivated,
" Ellipticsaid. "The vanity addresses used by the hackers are generated through 'brute-force' methods involvin
g the creation of large numbers of cryptographic key pairs until one contains the desired text.""But creating
vanity addresses with text strings as long as those used in this hack is computationally infeasible. This mean
s that Predatory Sparrow would not have the private keys for the crypto addresses they sent the Nobitex funds
to, and have effectively burned the funds in order to send Nobitex a political message."On June 19, 2024, the
pro-Israel grouppreleasedwhat it said was Nobitex's "full source code," after it's said to have stolen over $90
million in digital currency from the crypto exchange. Nobitex, in a series of posts on X, said the total valu
e of stolen assets is estimated to be around $100 million."The stolen assets were

transferred to a wallet with
a non-standard address composed of arbitrary characters an approach that deviates significantly from conventi
onal crypto exchange hacks," the companysaid, noting that the "situation is now under control.""These wallets
were used to burn and destroy user assets. It is clear that the intention behind this attack was to harm the p
eace of mind and assets of our fellow citizens under false pretenses."Nobitex has sincesaidthe "scope and impa
ct of the attack are more complex than initially estimated," and pointed out that the current internet disrupt
ions in the country and its limited on-site access due to the conflict have impacted its response efforts.Disc
over real-time defense tactics to detect and block deepfakes, fake domains, and multi-channel scams before the
y cause damage.We'll unpack how leading teams are using AI, privacy-first design, and seamless logins to earn
user trust and stay ahead in 2025.Get the latest news, expert insights, exclusive resources, and strategies fr
om industry leaders all for free.

Link: https://thehackernews.com/2025/01/donot-team-linked-to-new-tanzeem.html