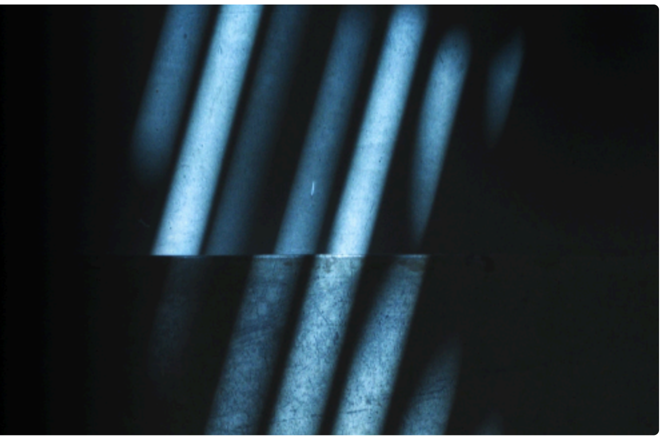
SPYWARE

TwoDash

15+ mentions in the last 2 weeks

62 articles in the last 12 months



Using open-source data collected by Feedly AI.

Overview

TwoDash is a type of malware deployed by Russian hackers for the purpose of gathering intelligence on targeted networks. It is used in conjunction with other malware, such as Waiscot and CrimsonRAT, to enhance their capabilities in cyber operations.

Aliases

- Two Dash

Source: Malpedia

Article count

No article counts found. Try changing the time period.

Top targeted industries and organizations

INDUSTRIES	ORGANIZATIONS	ARTICLES	ATTACK REPORTED
Others 1 article	• Storm-0156	1	5 days ago

Top threat actors using this malware

	Articles
Turla	12

Tactics, Techniques, and Procedures

Last mentioned

TECHNIQUE	MITRE ID	PROCEDURES	MITIGATION	ARTICLES

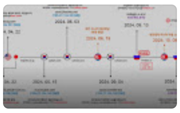
No TTPs available at the moment

Exploited vulnerabilities

CVE ID	CVSS SCORE ⬍	EPSS SCORE ⬍	VENDOR	PRODUCT	TREND	WEAPONIZED ⬍

No exploited vulnerabilities at the moment

News



CTO at NCSC Summary: week ending December 8th

Threat Actors • by Ollie Whitehouse / 2d • Threat Intelligence Reports • 2 CVEs • 27 TTPs

submitted by /u/digicat [link] [comments]

Also in r/cybersecurity, CTO at NCSC, +4 feeds

Russian Hackers Hijacked Pakistani Actor Servers For C2 Communication

New Malware > Waiscot • GBHackers Security by Aman Mishra / 3d • Command and Control (Enterprise TA0011) • Russian hackers exploit Pakistani servers

They have deployed their own malware, TwoDash and Statuezy, and leveraged Storm-0156's malware, Waiscot and CrimsonRAT, to gather intelligence on targeted networks, which […] The post appeared first on GBHackers Security

Also in Cyberattacks News, RSS reader not yet w..., +85 feeds

Russian Hacker Secret Blizzard Hijack C2 Infrastructure in New Espionage Campaign

4 TTPs • Cybersecurity News by do son / 3d • Original source: Lumen Blog / 5d • Turla exploits Pakistani hackers' servers

Using Storm-0156's infrastructure as a springboard, Secret Blizzard not only deployed their malware, including TwoDash and Statuezy, but also exploited this access to collect intelligence from networks compromised by Storm-0156.…

Also in Patrick C Miller, Techmeme, +81 feeds

Turla targets Pakistani APT infrastructure for espionage

2 TTPs • SCM feed for Latest by SC Staff / 4d • Original source: r/blueteamsec / 5d • Turla exploits Pakistani hackers' servers

After achieving initial access to a Storm-0156 C2 server in December 2022, Turla sought to take over more of the Pakistani threat operation's C2s to compromise Afghan government organizations' networks with the TwoDash downloader and…

Also in Patrick C Miller, Techmeme, +81 feeds

Frequent freeloader part I: Secret Blizzard compromising Storm-0156 infrastructure for espionage

Threat Actors • Threat intelligence by Microsoft Threat Intelligence / 4d • Threat Actors • Threat Intelligence Reports • IoC > 3 domains, 21 IPs, and 9 hashes

However, since October 2023, Secret Blizzard predominantly has been using a .NET backdoor that Microsoft Threat Intelligence refers to as TwoDash alongside a clipboard monitoring tool referred to as Statuezy.

Also in Patrick C Miller, Techmeme, +81 feeds

Russian Hackers Exploit Rival Attackers' Infrastructure for Espionage

9 TTPs • Infosecurity / 4d • Original source: r/blueteamsec / 5d • Turla exploits Pakistani hackers' servers

Russian cyber espionage group Secret Blizzard has used the tools and infrastructure of at least six other threat actors during the past seven years, according to Microsoft. The Microsoft researchers observed that Secret Blizzard…

Also in Patrick C Miller, Techmeme, +81 feeds

See 9 more articles and social media posts

Made with feedly