CYBERCRIME NEWS

ISSUE 22 • AUGUST 2026

INFOSTEALERS

WHAT ARE INFOSTEALERS?

MOST PEOPLE HAVE HEARD OF RANSOMWARE, BUT MANY HAVE NEVER HEARD OF "INFOSTEALER" MALWARE. INFOSTEALERS ARE A TYPE OF MALICIOUS SOFTWARE DESIGNED TO SECRETLY HARVEST SENSITIVE DATA SUCH AS PASSWORDS, FINANCIAL INFORMATION, BUSINESS CREDENTIALS AND MORE. BECAUSE THEY OPERATE COVERTLY, THEY ARE OFTEN VERY HARD TO DETECT.

HOW DO BUSINESSES BECOME INFECTED?

Like other malware, infostealers are commonly infected following:

- Phishing emails
- Fake software downloads
- Malicious browser extensions
- Pirated software
- Malicious advertising and fake CAPCHA websites.

Once installed, within seconds the software will begin harvesting and exfiltrating sensitive data.

WHY DO CRIMINALS USE INFOSTEALERS?

The data itself is valuable, but there is a secondary motive behind criminals using infostealers. Stolen credentials are often used to access company, financial, email, social media accounts, and cloud platforms to perpetuate further cybercrime and fraud.

Additionally, many cyber criminals operate as part of a wider criminal network, meaning exfiltrated data is often sold on.

In short, infostealers are popular because they allow criminals to steal trusted credentials, avoid many traditional security controls, and generate multiple opportunities for financial gain.

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

DORSET POLICE

PRODUCED BY DORSET OPCC AND DORSET POLICE

HOW TO PROTECT YOUR BUSINESS

There are many important measures an organisation can employ to prevent installation of malicious software.

• **Two Step Verification (2SV) / Multi Factor Authentication:** This is crucial for all organisations, big and small. 2SV offers an additional layer of security for online accounts, requiring a second piece of information alongside a password.

Without this secondary piece of information, usually a numerical code, access is denied. Therefore, even if password credentials are stolen, the account remains inaccessible.

• **Use a password manager** as opposed to saving passwords in a browser. However, do ensure research is conducted on the password manager, such as on confidentiality, data, and privacy privacies.

• **Ensure devices, software, and Operating Systems (OS) are updated** as soon as an update becomes available.

• **Train staff** to recognise signs of phishing and Business Email Compromise – We can help with this.

CLOSING THOUGHTS

Cyber criminals do not always need to hack your systems when they can access accounts with stolen credentials. By strengthening account security and improving staff awareness, businesses can significantly reduce the risk posed by infostealer malware.

Dorset Police offer free Cyber Awareness sessions, tailored to your businesses' needs. For more information on the sessions we offer, please contact Hannah Bird, Cyber Crime Protect and Prevention Officer at **cybercrimeprevention@dorset.pnn.police.uk**

DORSET POLICE

Dorset Police

Force Headquarters
Winfrith, Dorchester
Dorset DT2 8DZ

E cybercrimeprevention@dorset.pnn.police.uk
www.dorset.police.uk

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

Office of the Dorset Police & Crime Commissioner

Force Headquarters
Winfrith, Dorchester
Dorset DT2 8DZ

T 01202 229084
E pcc@dorset.pnn.police.uk
www.dorset.pcc.police.uk