FOURTH DIMENSION TECHNOLOGIES INC

Cyber Attacks 2024

fourdtech.com | info@fourdtech.com

FOURTH
DIMENSION
expect more

Highlights

Key events we will be discussing:

- **New Malware Alert: SamsStealer on the Rise!**
- FakeBat Loader Malware Incident
- Mailcow Flaw Incident
- Pegasus Virus

1

New Malware Alert: SamsStealer on the Rise!

We are witnessing the emergence of a new .NET based malware named "SamsStealer." Spreading through Telegram, this malicious software targets Windows systems, aiming to steal sensitive files. With its advanced evasion techniques and leveraging a popular messaging platform, SamsStealer poses a significant threat.

Key Points:

NAME:

SamsStealer

TYPE:

.NET Malware

TARGET:

Windows Operating Systems

DISTRIBUTION METHOD:

Telegram

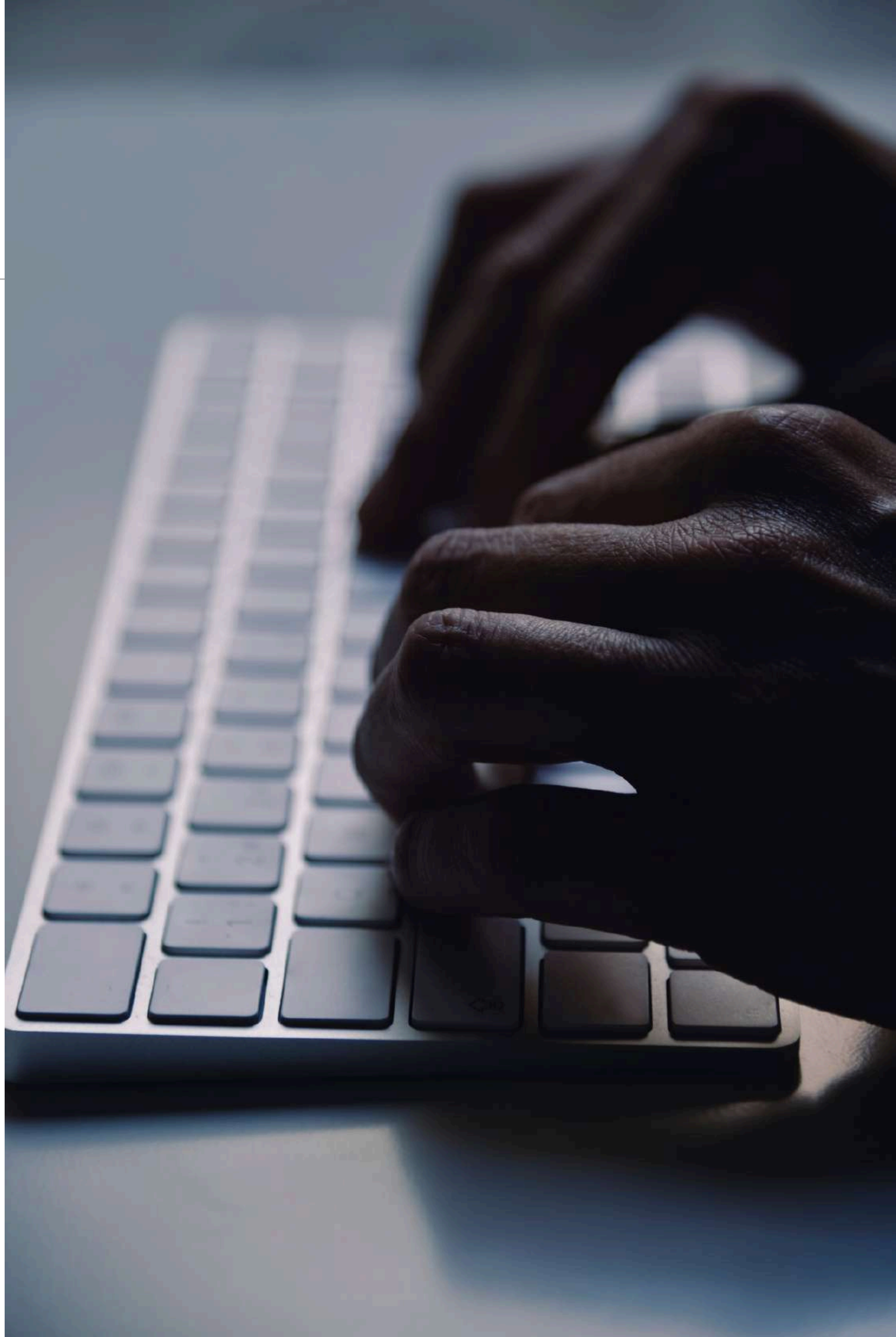
info@fourdtech.com

How It Works:

SamsStealer creates a temporary folder and proceeds to steal passwords, cookies, and other information from browsers like Chrome and Edge, as well as cryptocurrency wallets.

Techniques Used:

T1041: Exfiltration over the C2 Channel
T1082: System Information Discovery
T1566.001: Spearphishing Attachment
T1567: Exfiltration Over Web Service
T1204.002: Malicious File
T1566: Phishing
T1005: Data from the Local System
T1204: User Execution



Capabilities:

- **Directory Scanning:** Searches user directories for specific types of files.
- **Data Exfiltration:** Compresses, encrypts, and securely sends stolen files to the attacker's server.

Evasion Tactics:

- **Code Obfuscation:** This malware hides its code to complicate analysis.
- **Anti-Analysis:** It detects virtual environments or debugging tools and alters behavior to avoid detection.

Potential Risks:

- **Data Breach:** Theft of sensitive information.
- **Financial Loss:** Stolen financial documents can cause direct monetary loss or fraud.
- **Reputation Damage:** Leaked data harms the reputation of an organization.

Mitigation Strategies:

- User Awareness Training: Educate users on the risks of downloading files from untrusted sources, especially on platforms like Telegram.
- Endpoint Protection: Implement strong endpoint protection solutions to detect and block .NET malware.
- Regular Backups: Ensure you regularly backup critical data and prevent data loss in case of an infection.
- Network Monitoring: Monitor network traffic for unusual activities that could indicate data exfiltration.

References:

cybersecuritynews | otx.alienvault.com | cyfirma.com

fourdtech.com | info@fourdtech.com