Malware analysis reports

National Cyber Security Centre ⋮ 2-3 minutes ⋮ Invalid Date

NCSC malware analysis reports (MARs) help network defenders understand selected malware threats in more technical depth, and provide indicators and TTPs to support threat hunting or modelling.

The reports focus on the technical detail features, components and structure of malware samples. We may also include analyst commentary to highlight notable techniques or approaches, but because of the risks around malware reuse and misinformation campaigns, MARs avoid statements on attribution or use by adversaries.

Sometimes reports may accompany wider NCSC advisories, which may explore adversaries and attribution.

While the NCSC makes every effort to assure the quality and accuracy of indicators and signatures, we remind you to use at your own risk and carry out your own validation before deploying them.

Line Dancer

In-memory shellcode loader targeting Cisco Adaptive Security Appliance (ASA) devices.

Published: 24/04/2024

- Report (PDF)
- YARA

Line Runner

A Lua webshell targeting Cisco Adaptive Security Appliance (ASA) devices and abusing CVE-2024-20359 for persistence.

Published: 24/04/2024

- Report (PDF)

Infamous Chisel

A collection of components associated with Sandworm designed to enable remote access and exfiltrate information from Android phones.

Published: 31/08/2023

- Report (PDF)
- YARA
- Indicators

Smooth Operator

MacOS supply chain malware that exfiltrates victim data using a custom data encoding algorithm over HTTPS.

Published: 29/06/2023

- Report (PDF)
- STIX
- YARA
- Indicators

Jaguar Tooth

Cisco IOS malware that collects device information and enables backdoor access.

Published: 18/04/2023

- Report (PDF)
- STIX
- Yara
- Snort

Small Sieve

Telegram Bot API based Python backdoor with file download and execution capability.

Published: 27/01/2022

- Report (PDF)
- STIX
- Indicators

Jolly Jellyfish

Non-persistent downloader for shellcode embedded in image files.

Published: 15/12/2021

Updated: 15/12/2022

- Report (PDF)
- STIX
- Yara
- Indicators

Infinite Second

PowerShell dropper used to deploy ComRAT.

Published: 03/09/2021

- Report (PDF)
- STIX
- Yara

Devil Bait

Malicious macro-enabled Microsoft Word document and VBScript.

Published: 03/08/2021

Updated: 20/09/2021

- Report (PDF)
- STIX
- Yara
- Sigma