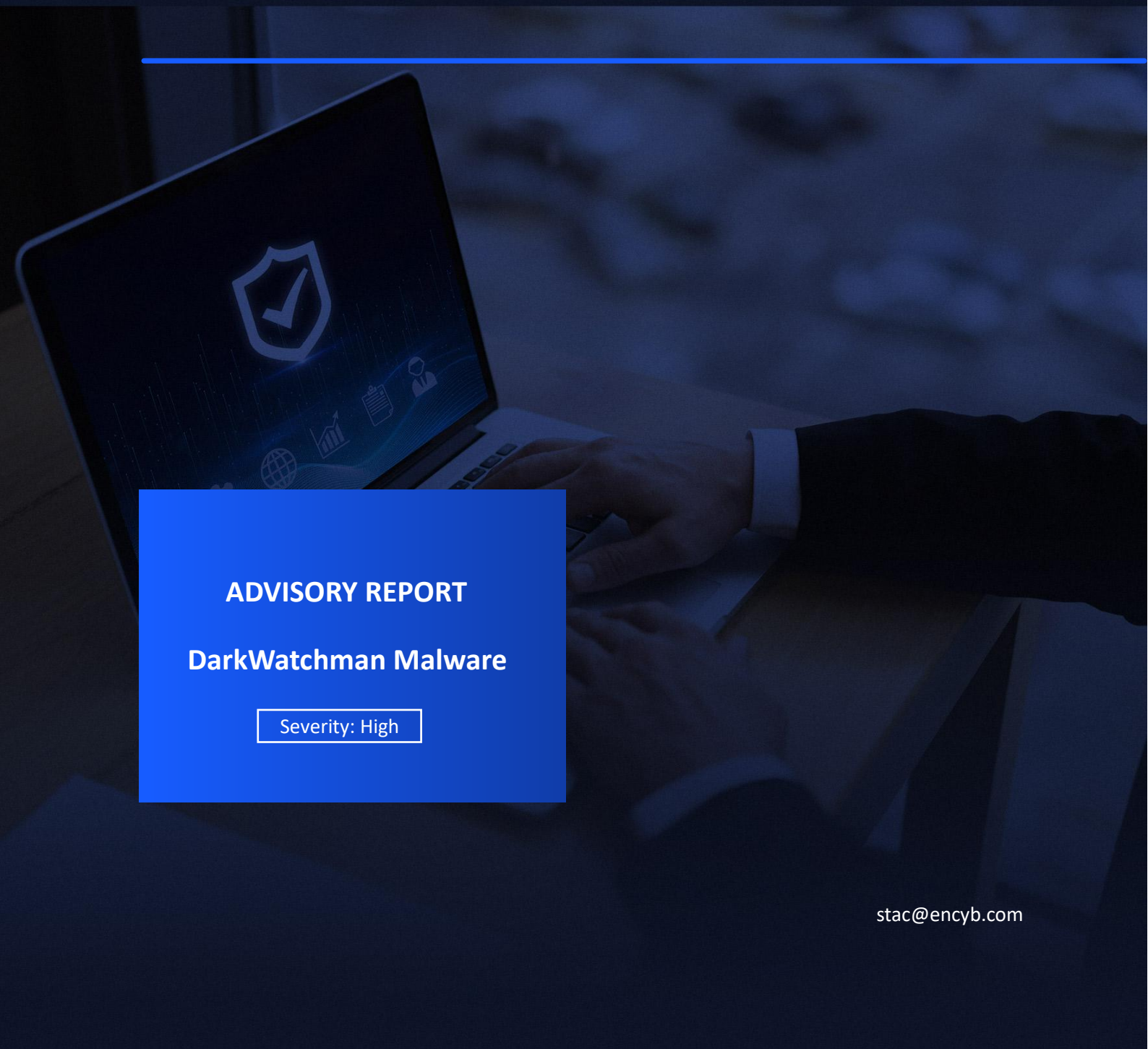
EnCyb

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.



ADVISORY REPORT

DarkWatchman Malware

Severity: High

stac@encyb.com

OVERVIEW

Darkwatch is a sophisticated Remote Access Trojan (RAT) and surveillance-focused malware family designed to establish persistent access to infected systems. Darkwatch has been associated with advanced cybercrime groups leveraging it for espionage, credential theft, and lateral movement across enterprise environments. The malware is typically distributed via spear-phishing campaigns, malicious installers, and compromised websites. Its modular architecture enables attackers to deploy additional payloads, capture sensitive user activity, and maintain long-term covert operations.

TECHNICAL DETAILS

1. Malware Type

- Darkwatch – Remote Access Trojan (RAT) / Surveillance Malware.

2. Infection Vectors

- Spear-phishing emails with malicious attachments or links.
- Trojanized software installers and cracked applications.
- Drive-by downloads from compromised or malicious websites.
- Malvertising campaigns leveraging exploit kits.

3. Capabilities

- Keylogging and screen capturing for surveillance.
- Credential theft from browsers, VPNs, and enterprise applications.
- Remote command execution and file exfiltration.
- Privilege escalation to maintain persistence.
- Deployment of secondary payloads (including ransomware or miners).
- C2 communication with encrypted channels to avoid detection.

4. Command & Control (C2)

- Darkwatch communicates via HTTPS and WebSockets, often using domain fronting or fast-flux DNS to disguise traffic. Exfiltrated data is compressed, encrypted, and rotated across multiple C2 nodes to evade takedown.

MITRE MAPPING

Tactic	Technique ID	Technique Name
Initial Access	T1566.001	Spear phishing Attachment
Initial Access	T1189	Drive-by Compromise
Execution	T1059.003	Windows Command Shell
Persistence	T1547.001	Registry Run Keys / Startup Folder
Defence Evasion	T1027	Obfuscated Files or Information
Defence Evasion	T1217	Obfuscated Files or Information
Credential Access	T1555.003	Credentials from Web Browsers
Credential Access	T1003.001	LSASS Memory Dumping
Discovery	T1082	System Information Discovery

Collection	T1056.001	Keylogging
Exfiltration	T1041	Exfiltration Over C2 Channel
Command and control	T1573.001	Encrypted Channel
Command and control	T1071.001	Application Layer Protocol: Web Protocols

IMPACT

- **Credential Theft**: Theft of enterprise credentials, VPN access, and privileged accounts.
- **Data Exfiltration**: Sensitive documents, intellectual property, and user activity logs may be stolen.
- **Operational Risk**: Attackers may achieve lateral movement and persistence, enabling espionage or ransomware staging.
- **Financial Loss**: Stolen credentials may be used for fraud, ransom demands, or access sold on dark markets.
- **Reputation Damage**: Breaches involving Darkwatch can undermine customer trust and regulatory compliance.

IOCs

Indicator Type	IOC
SHA256	b21098613cbc70c32c2c38bbbc7151436f8c8b6960b4855d378f96f875a4db10
SHA1	b3d169a505de6f452e38977af9844dab6f460d4f
MD5	a3b4eee33ef8051a0bbd59fef6325521

Recommendations

- Isolate infected hosts and block known IOCs.
- Apply latest OS and application security patches.
- Disable or restrict installation of unauthorized applications.
- Reset all passwords for accounts accessed from infected systems.
- Enforce Multi-Factor Authentication (MFA).
- Train employees on phishing recognition and malicious file indicators.
- Maintain offline, immutable backups of critical systems.
- Test recovery procedures to ensure resilience

References

- Analysis Report · CAPE Sandbox
- VirusTotal - File - b21098613cbc70c32c2c38bbbc7151436f8c8b6960b4855d378f96f875a4db10