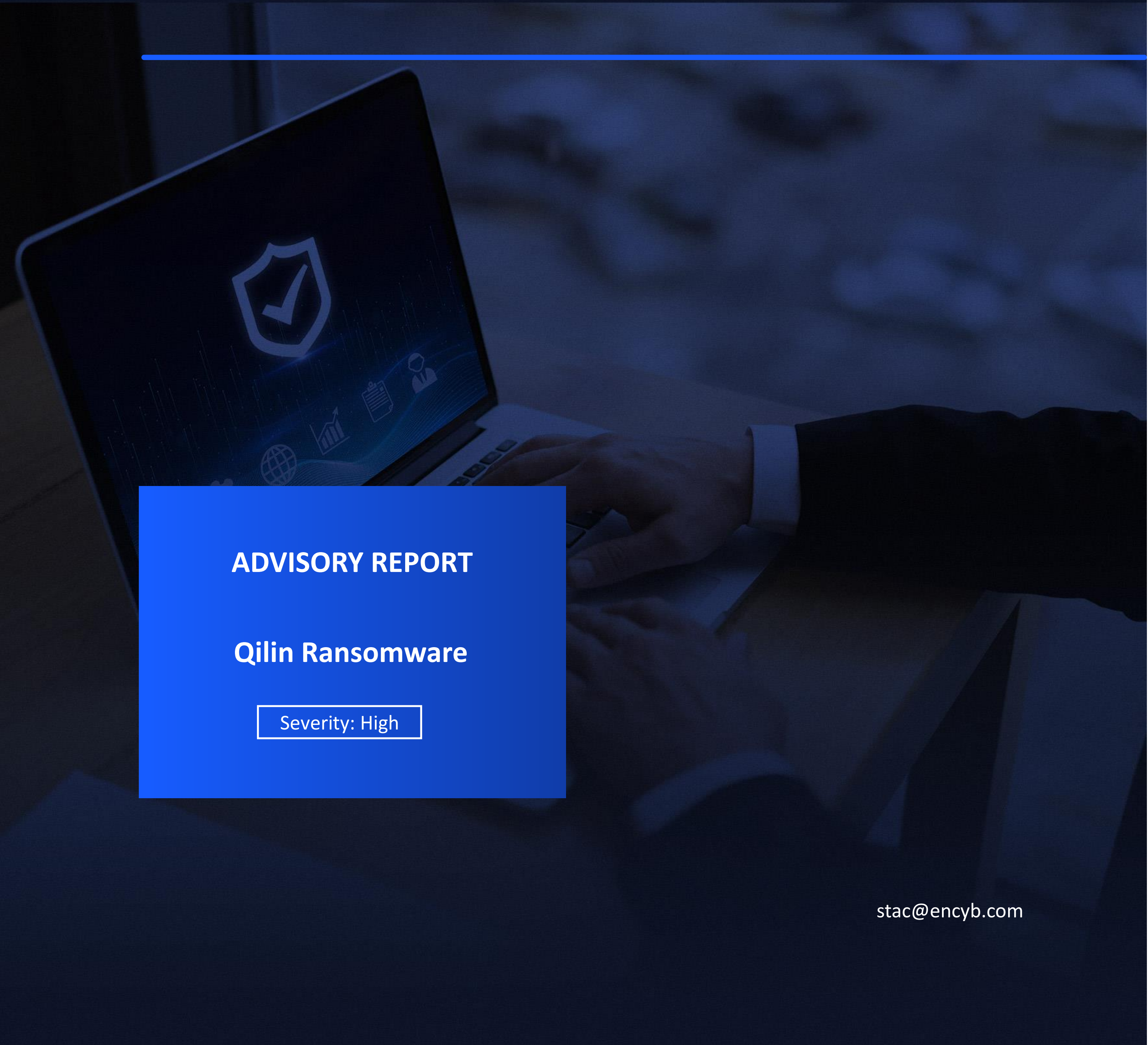
EnCyb

SECURITY THREAT ADVISORY COUNCIL (STAC)

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



ADVISORY REPORT

Qilin Ransomware

Severity: High

stac@encyb.com

OVERVIEW

Qilin (also tracked as Agenda / Gold Feather / Water Galura) has evolved its operational playbook to include a hybrid attack model that combines a Linux-compiled ransomware payload executed on Windows hosts together with a "Bring Your Own Vulnerable Driver" (BYOVD) technique to disable/hamper endpoint protection.

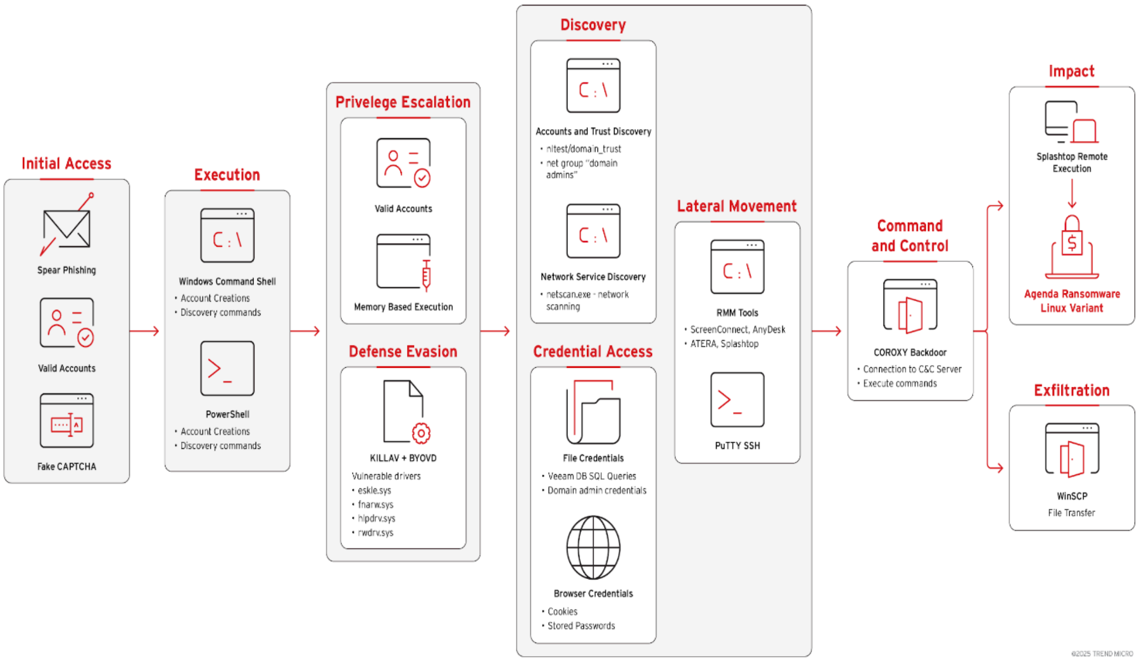
TECHNICAL DETAILS

- **Initial Access:** Credential theft (phishing, reuse of credentials, leaked credentials, Fake CAPTCHA), compromised RMM tools and remote-access products.
- **Lateral Movement & Escalation:** Abuse of legitimate remote management tools (AnyDesk, Splashtop, MeshAgent, WinSCP, RMM suites) and elevated credentials to move laterally and access backup systems and hypervisors.
- **Defense Evasion (BYOVD):** Deployment of a signed but vulnerable kernel driver (reported as variants such as TPwSav.sys in observed cases) to disable or tamper with endpoint detection and response (EDR) functionality, allowing execution of otherwise-detected payloads.
- **Cross-platform Execution:** Transfer and execution of a Linux-compiled ransomware binary on Windows hosts using legitimate utilities (file transfer + remote execution) so the binary runs under a compatible runtime or through helper tools, evading Windows-specific detection signatures.
- **Impact Activities:** Encryption of target data, deletion of Volume Shadow Copies (VSS), event log clearing, credential harvesting, and exfiltration of sensitive data before encryption.

MITRE MAPPING

TACTIC	TECHNIQUE ID	TECHNIQUE NAME
Initial Access	T1078	Valid Accounts
Initial Access	T1566	Phishing
Execution	T1059	Command and Scripting Interpreter
Persistence	T1547	Boot or Logon Autostart Execution
Privilege Escalation	T1068	Exploitation for Privilege Escalation
Defense Evasion	T1218	Signed Binary Proxy Execution
Defense Evasion	T1562.001	Impair Defenses: Disable or Modify Tools
Lateral Movement	T1021	Remote Services
Collection	T1555	Credentials from Password Stores
Exfiltration	T1041	Exfiltration Over C2 Channel
Impact	T1486	Data Encrypted for Impact
Impact	T1490	Inhibit System Recovery

ATTACK CHAIN



IMPACT

- Potential full-disk or wide-scale file encryption across enterprise shares and servers.
- Backup corruption or deletion due to backup credential theft and VSS deletion, complicating recovery.
- Severe operational disruption, regulatory exposure, and reputational damage if exfiltrated data is published.

IOCs

INDICATOR TYPE	IOC
IP Address	86.106.85.36
MD5	719ba3d7051173982919d1e4e9e9a0ec
SHA-1	75ebd5bab5e2707d4533579a34d983b65af5ec7f
MD5	227f14f4c3aa35b9fb279f52c73b2e1e
MD5	bb8bdb3e8c92e97e2f63626bc3b254c4
SHA-1	70df765f554ed7392200422c18776b8992c09231
C2/ Payload Servers	5[.]221[.]64[.]245/mot/
C2/ Payload Servers	104[.]164[.]55[.]7/231/means.d
Executable	2stX.exe
Executable	Or2.exe
Executable	cg6.exe

Executable	44a.exe
Executable	aa.exe
Driver	eskle.sys
Driver	rwdrv.sys
Driver	hlpdrv.sys

Recommendations

- Enable MFA for all remote access and privileged accounts, rotate service account credentials regularly.
- Enforce driver signing policies and restrict driver installation to authorized change windows and inventory managed drivers**.**
- Allowlisting/Application Control: Consider allowlisting for critical systems to prevent execution of unexpected binaries, including ELF/foreign-format files on Windows hosts.
- Isolate backup infrastructure and critical systems from general user networks.

REFERENCES

- https://thehackernews.com/2025/10/qilin-ransomware-combines-linux-payload.html
- https://securityaffairs.com/183891/malware/linux-variant-of-qilin-ransomware-targets-windows-via-remote-management-tools-and-byovd.html
- https://otx.alienvault.com/browse/global/pulses?q=Qilin%20ransomware&include_inactive=0&sort=-modified&page=1&limit=10&indicatorsSearch=Qilin,ransomware