THE UNITED REPUBLIC OF TANZANIA
TANZANIA COMMUNICATIONS REGULATORY AUTHORITY
ISO9001:2015 CERTIFIED

SECURITY ADVISORY

CYBER ATTACKS ON CRITICAL INFORMATION INFRASTRUCURE (CII)

1.0. INTRODUCTION

Tanzania Computer Emergency Response Team (TZ-CERT), established under Tanzania Communications Regulatory Authority (TCRA), is aware of a cyber-attack targeting organizations with Critical Information Infrastructure (CII)[1]. The threat actors are reported to use a new variant of ransomware referred to as "DarkSide" to lock down computer systems and ask the victims to pay them money in exchange for unlocking keys. Apart from locking down victims' computer systems, the threat actors also steal sensitive corporate data for malicious intentions.

One of the recent high-profile attacks is the shutdown of the fuel supply system of a major pipeline company based in the United States (US), which resulted in acute fuel shortages and inflation across the country.

Pursuant to section 6(s) of the **Electronic and Postal Communications (CERT) Regulations 2018**, TZ-CERT is mandated to proactively provide early warning on eminent cybersecurity incidents. Keeping that in mind, this advisory has been prepared to advise critical information infrastructure (CII) institutions to adopt a heightened state of awareness and implement recommendations listed in the mitigation section in this advisory to protect themselves from and better respond to DarkSide attacks.

2.0. TECHNICAL DETAILS

DarkSide is ransomware-as-a-service (RaaS) malware. The malware developers are reported to secure some of their money from other ransomware-spreading cyber criminals known as affiliates. This strategy made it easier for the malware to spread quickly around the world. As of August 2020, DarkSide actors have been targeting CII organizations to **disrupt critical business operations** and **steal confidential data**. Unlike other actors, DarkSide actors target high-income institutions that can afford to pay a ransom if infected.

[1] According to the **Cybercrimes Act 2015,** Critical Information Infrastructure (CII) include assets, devices, information systems, communication networks, whether physical or virtual so vital to the United Republic of Tanzania (URT) that their incapacitation affect national security or the economy and social wellbeing of citizens.

According to open-source reporting, DarkSide actors have previously been observed gaining initial access to targets through **phishing** and exploiting remotely accessible accounts and systems. DarkSide actors have also been observed using **Remote Desktop Protocol (RDP)** to maintain persistence.

After gaining access, DarkSide actors deploy the malware to encrypt and steal sensitive data and after that, demand the victims a ransom in exchange for a decryption key. The actors may also threaten victims to publicly publish their data if the ransom is not paid. Further analysis revealed that the ransomware uses **Salsa20**[2] and **RSA**[3] algorithms to encrypt compromised files and folders. For Command and Control (C&C) functions, the DarkSide ransomware uses The Onion Router (TOR)[4] and Cobalt Strike[5].

In the early stages, the DarkSide ransomware employs stealthy techniques to propagate into target systems. Their actors also employ reconnaissance to ensure that their attack tools and techniques evade detection on endpoints.

3.0. INDICATORS OF COMPROMISE (IOCs)

Kindly refer to **Annex I** to this advisory to obtain an updated file hash Indicators of Compromise (IoC) published on 20th May, 2021 by Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI).

4.0. MITIGATIONS

TZ-CERT urges CII owners and operators to apply the following mitigation measures to reduce the risk of DarkSide attacks: -

4.1. Implement **network segmentation** to minimize the damage of a successful DarkSide attack.

4.2. Implement strong **spam filters** to prevent phishing emails from reaching end users.

4.3. Implement **multi-factor authentication** for remote access to in-house systems and local area networks.

4.4. Filter emails containing executable files from reaching end-users' mailbox.

[2] **Salsa20** is a modern and efficient hash function that works on data blocks of size of 64 bytes.

3 Rivest-Shamir-Adleman – RSA, is a public-key cryptosystem that is widely used for secure data transmission.

[4] **The Onion Router (TOR)** is free and open-source software for enabling anonymous communication by directing Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays in order to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis.

[5] **Cobalt Strike** is a commercial, full-featured, remote access tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors". Cobalt Strike's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.

4.5. Consider implementing centralized patch management to ensure that all software and applications in your network are up to date.

4.6. Perform user **awareness on phishing attacks** and their countermeasures to avoid infecting their machines with malware through visiting malicious websites or opening malicious attachments.

4.7. Restrict remote access to the network resources, mainly by limiting Remote Desktop Protocol (RDP). If deemed so, restrict the originating sources and implement multi-factor authentication.

4.8. Implement robust data backup and recovery strategy to help prevent disruption of critical business operations in the event of DarkSide attack.

4.9. Implement Intrusion Detection and Prevention System (IDS/IPS) to prohibit inbound and outbound communications with known malicious traffics.

4.10. Implement and enforce an effective security policy to mitigate security risks resulting from use of personally owned devices at the workplace; example, "Bring Your Own Device" (BYOD) policy to manage personal devices connecting to the institutional network.

4.11. Block indicators of compromise from the IOC list at the firewall.

4.12. Ensure user and process accounts are limited through account use policies, user account control, and privileged account management. Organize access rights based on the principles of least privilege and separation of duties.

4.13. Set antivirus/antimalware programs to conduct regular scans of IT network assets using up-to-date signatures.

4.14. Implement unauthorized execution prevention by: -

a) Disabling macro scripts from Microsoft Office files transmitted via email.

b) Implementing application allowlisting, which only allows systems to execute programs known and permitted by security policy. Implement software restriction policies (SRPs) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular internet browsers or compression/decompression programs, including the *AppData/LocalAppData* folder.

4.15. Configure your network to detect and/or block inbound connection from "TOR", Cobalt Strikes servers and other post exploitation tools.

In case your organization is hit by a DarkSide ransomware, TZ-CERT recommends the following actions: -

4.16. Remove the infected system from your network, and disable the computer’s wireless, Bluetooth, and other potential networking capabilities.

4.17. Shut down and disconnect any other computer or device that is sharing a network with the infected computer that has not been fully encrypted with ransomware.

4.18. Use secure backups. Ensure that your backup data is offline and secure all the time. If possible, scan your backup data with an antivirus program to check that it is free of malware.

5.0. IMPORTANT NOTICE

TZ-CERT advises victims not to pay ransom to DarkSide actors when requested. Doing so may encourage actors to continue launching attacks on other organizations, promote other criminals to participate in the spread of the malware, and / or fund illegal activities. **Paying the ransom does not guarantee that encrypted files will be restored**.

6.0. REFERENCES

a) https://us-cert.cisa.gov/ncas/alerts/aa21-131a
b) https://www.colpipe.com/news/pressreleases/media-statement-colonial-pipeline-system-disruption
c) https://otx.alienvault.com/pulse/60821a187be8d208269c103c/

CONTACTS:

If you encounter a cybersecurity incident and need a technical assistance, please contact TZ-CERT through: -

Tanzania Computer Emergency Response Team (TZ-CERT)
Mawasiliano Towers, 20 Sam Nujoma Road
P.O Box 474
14414, DAR ES SALAAM
Phone: +255 22 2199760-9
Fax: +255 22 2412009 / +255 22 2412010
Email: info@tzcert.go.tz / incidents@tzcert.go.tz
PGP Key id: EED630F6
PGP Fingerprint: 0A1C CF48 D623 9BE7 676B 4C03 EF91 6FCA EED6 30F6

Annex I

INDICATORS OF COMPROMISE FOR DARKSIDE RANSOMWARE

TYPE	INDICATOR	TITLE
FileHash-MD5	*987b65cd9b9f4e9a1afd8f8b48cf64a7*	*pchunter64.exe*
FileHash-SHA1	*5f1cbc3d99558307bc1250d084fa968521482025*	*pchunter64.exe*
FileHash-SHA256	*2b214bddaab130c274de6204af6dba5aeec7433da99aa950022fa306421a6d32*	*pchunter64.exe*
FileHash-SHA256	*5467a0aa064d7340031e9087cdbdacc2c656c80a458a913889f308056533d9eb*	*file.exe*
FileHash-MD5	*8a4e27cd31a3795e17e84e25da524e80*	*Test (3).exe*
FileHash-SHA1	*62d8735539d102f92a8a30b15a94e242bff3613e*	*Test (3).exe*
FileHash-SHA256	*b43bde75780244aeee719ae926c1f901291574c9400b5e6d0c2fdc135d0c6fe5*	*Test (3).exe*
FileHash-MD5	*ebfd9b1f421fac88db43e1ea8d67ad52*	*KAAV.EXE*
FileHash-SHA1	*d78fd52d7693b137f0cc3d56a77f5ec83c949575*	*gift.exe, gift1.exe*
FileHash-SHA1	*d6b7ebde993a9c4bc6adfa83dcc7fc4528bd2db3*	*asn.bat*
FileHash-MD5	*979692cd7fc638beea6e9d68c752f360*	*acer.exe*
FileHash-SHA1	*c511ae4d80aaa281c610190aa13630de61ca714c*	*acer.exe*
FileHash-SHA256	*0a0c225f0e5ee941a79f2b7701f1285e4975a2859eb4d025d96d9e366e81abb9*	*acer.exe*
FileHash-SHA1	*a14afbb27e7a9bd2740547427b7cdfc7d6548a92*	*spoolsv.exe*
FileHash-SHA1	*9e1ee72ca493d9658d01910b2aea5a3728dee9e3*	*reconfig.exe, one.exe, spoolsv.exe, gift2.exe*
FileHash-SHA1	*9d2c297e9c185d30da1920e995eb13fe16562493*	*Ech.exeCrc.exe*
FileHash-SHA1	*7769cea037ebf692f1d94bab37aaa9d01c5db0dd*	*winrun.exe*
FileHash-SHA1	*7165647de8e84715299f177e7c840cabbd149763*	
FileHash-MD5	*e9dc058440d321aa17d0600b3ca0ab04*	*g.exe*
FileHash-SHA1	*539c228b6b332f5aa523e5ce358c16647d8bbe57*	*g.exe*
FileHash-SHA256	*e8a3e804a96c716a3e9b69195db6ffb0d33e2433af871e4d4e1eab3097237173*	*g.exe*
FileHash-SHA1	*3d202aa6ad8cdccde1d59b5e3dab162f5fcbeda3*	*asn.bat*
FileHash-MD5	*91889658f1c8e1462f06f019b842f109*	*zero.exe*
FileHash-SHA1	*33a6b39fbe8ec45afab14af88fd6fa8e96885bf1*	*zero.exe*
FileHash-SHA256	*36bc32becf287402bf0e9c918de22d886a74c501a33aa08dcb9be2f222fa6e24*	*zero.exe*
FileHash-SHA1	*1f028ea7ae00bac06fe190482f9171f38b45d0d6*	*spoolsv.exe*
FileHash-SHA1	*1e0aa7aaeb8bddd03254f0c4cd0193268b132e4d*	*9ibrT.exe*
FileHash-SHA1	*1b7172ec213997ed02ce1bf6dacb722f44a00576*	*zero.exe*
FileHash-SHA1	*13e2024d8b31b96f4617b62bf4eb8e9c9bf8f*	

	2f5	
FileHash-SHA1	0d35e1eab210859d746032b6200db0d74e45a6bc	
FileHash-MD5	0842f6de2f20e102a276030e0ad216d5	svchost.exe
FileHash-SHA1	08d1da979f8d568b62701d7cedf1d0e81b7bab4d	svchost.exe
FileHash-SHA256	b9d60d450664c1e8fbfd6b2ec58fdeb2fd81797e183906a4536b59bc4f79846f	svchost.exe
FileHash-MD5	ea3999af92a594402471748374a468fc	64.exe
FileHash-SHA1	142ab367d5f83018d30c3d17b9dd87f2e35eba08	64.exe
FileHash-SHA256	b1c7872598053eb2fd07b0eabe223cbccef2edd2e403255b5ab8646e32124862	64.exe
FileHash-MD5	e2ed793ded71e097436f5829a42f96d9	def.bat
FileHash-MD5	e1ccabd83ec346cd9794c94801c6e6ab	Nsd.exe
FileHash-MD5	c1174225533b6db2d1e078b2eaa19028	Sk.exe
FileHash-MD5	b4a9c9eb091a81a65162c1f7957bded4	Azure_agent.exe.exe
FileHash-MD5	a8920685634d5793b2937510b2881e40	acer.exe
FileHash-MD5	a82b44581f7c7b70d7ec32411ba44d46	Cyls.bat
FileHash-MD5	9e1fd4f7f9c8fc94afc2b2024ade44f5	Ar2.exe
FileHash-MD5	954f9876d93fa5d3dde3c1fd89872f2a	file.exe
FileHash-MD5	897fd2e61928417881089e492639f58f	Release.exe
FileHash-MD5	8750c7aba06a7188c227254e0515a954	Vnzoz__d137__2743686099491__1612727785_1.exe
FileHash-MD5	8079676dd62582da4d2e9d2448c1142d	d.exe, d3.exe
FileHash-SHA1	3ed7c6f0f90e176eeca091ebe8528fba10603d51	d.exe, d3.exe
FileHash-SHA256	f7eda7111ac0f95dfbd817bd0962defe35412de12964f178421122e96c72495b	d.exe, d3.exe
FileHash-MD5	73f2bef2d5bad58106825e0fbe18aecd	134c.exe
FileHash-MD5	6af99fd0c053ca096d3fc61e41f1d07a	Desktop.exe
FileHash-SHA1	06856cab5b85104788d679bbbb75d270a90eabb0	Desktop.exe
FileHash-SHA256	6184e4c8915a3924a9a12e26c42cffef35a1d1380a8c0a236ef65df71b20c217	Desktop.exe
FileHash-MD5	65e801948737814b76dfb4fa3975f311	134.exe
FileHash-MD5	653b8fc4f8e937dac82291a46fc0981f	FULL.exe
FileHash-MD5	577a1311362ab64dd86f14c7e6fdb319	info.exe; Gg.exe; inf.exe; info1.exe
FileHash-MD5	46b157174c970dfe9d4fa71ba3ad9dba	Installer.exe
FileHash-MD5	464305094d4cbf567e2b8b64471d5f8e	README.00000000.TXT
FileHash-MD5	463dc22be6298fdbb0181be362615edd	reconfig.exe, one.exe, spoolsv.exe
FileHash-MD5	394b17f84fc6c0ce40fccb800130153b	gift.exe, gift1.exe
FileHash-MD5	2f4159dda4f5192d8cfd2dc3432c981f	def.bat
FileHash-MD5	29372529b316373d55eae430ed710815	134b.exe
FileHash-MD5	2491ce6f5fcc8bb20ea4c60e094390b0	
FileHash-MD5	224e5c3a7521c2a98d03f1e5086ed50c	134a.exe
FileHash-MD5	216c9eced26bc6c7b1af175c585df26b	_2021-02-21_03-13.exe, Gd.exe, Sd.exe, Info.exe, Infa.exe
FileHash-MD5	18ea49336cade89c161c5975fda7cd6f	1.exe
FileHash-MD5	1716c6a315ce64edc532f05906c3d704	Host-test.exe
FileHash-SHA1	2269cdc706b412d55749dd7b8a8b7cc14ce83532	Host-test.exe
FileHash-SHA256	ca77f63a08f4e01e7e7294695eb300610e65f22333256d547d0125075bed2cc8	Host-test.exe

FileHash-MD5	*131eff5622870f73f00c7f16c0646991*	*Skc.exe*
FileHash-MD5	*1210dcbfbb8532f25bafdda862ff2177*	
FileHash-MD5	*08646478a2ba16fa350a650e03bd115f*	*Setup.exe*
FileHash-MD5	*02ea21db281a790aa7dfecb6355d2572*	*stop.bat*
FileHash-MD5	*262bc500b93b5238c6715543bdf6638e*	*9ibrT.exe*
FileHash-MD5	*b278d7ec3681df16a541cf9e34d3b70a*	*homie.exe*
FileHash-SHA1	*666a451867ce40c1bd9442271ef3be424e2d9b17*	*homie.exe*
FileHash-SHA256	*bafa2efff234303166d663f967037dae43701e7d63d914efc8c894b3e5be9408*	*homie.exe*
FileHash-MD5	*4d3d3919dda002511e03310c49b7b47f*	*grabff.exe*
FileHash-SHA1	*b16a1eb8bc2e5d4ded04bfaa9ee2b861ead143ba*	*grabff.exe*
FileHash-SHA256	*7d57e0ba8b36ec221b16807ce4e13a1125d53922fa50c3827a5ebd6811736ffd*	*grabff.exe*
FileHash-MD5	*d6a246a98a0387e2a5f9d95ddd8ae164*	*Netscan.exe; syspool.exe*
FileHash-SHA1	*9d39c0d21b96ebb210fe467ad50604f05543db8e*	*Netscan.exe; syspool.exe*
FileHash-SHA256	*459d655c416cc429a7661c0dddc3826a6b34cce0c662ccd8db735934858aa010*	*Netscan.exe; syspool.exe*
FileHash-MD5	*c81dae5c67fb72a2c2f24b178aea50b7*	*ut.exe*
FileHash-SHA1	*4bd6437cd1dc77097a7951466531674f80c866c6*	*ut.exe*
FileHash-SHA256	*48a848bc9e0f126b41e5ca196707412c7c40087404c0c8ed70e5cee4a418203a*	*ut.exe*
FileHash-MD5	*f87a2e1c3d148a67eaeb696b1ab69133*	*acer.exe*
FileHash-SHA1	*d1dfe82775c1d698dd7861d6dfa1352a74551d35*	*acer.exe*
FileHash-SHA256	*9cee5522a7ca2bfca7cd3d9daba23e9a30deb6205f56c12045839075f7627297*	*acer.exe*
FileHash-MD5	*27304b246c7d5b4e149124d5f93c5b01*	*psexec; psexec.exe; MEGA_x64_Rus_Setup.exe; PsExec.exe; psexec.exe; pse.exe*
FileHash-SHA1	*e50d9e3bd91908e13a26b3e23edeaf577fb3a095*	*psexec; psexec.exe; MEGA_x64_Rus_Setup.exe; PsExec.exe; psexec.exe; pse.exe*
FileHash-SHA256	*3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef*	*psexec; psexec.exe; MEGA_x64_Rus_Setup.exe; PsExec.exe; psexec.exe; pse.exe*