Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:123 **31-12-2020**

Name: New Worm targeting both Linux and Windows Servers

Summary:

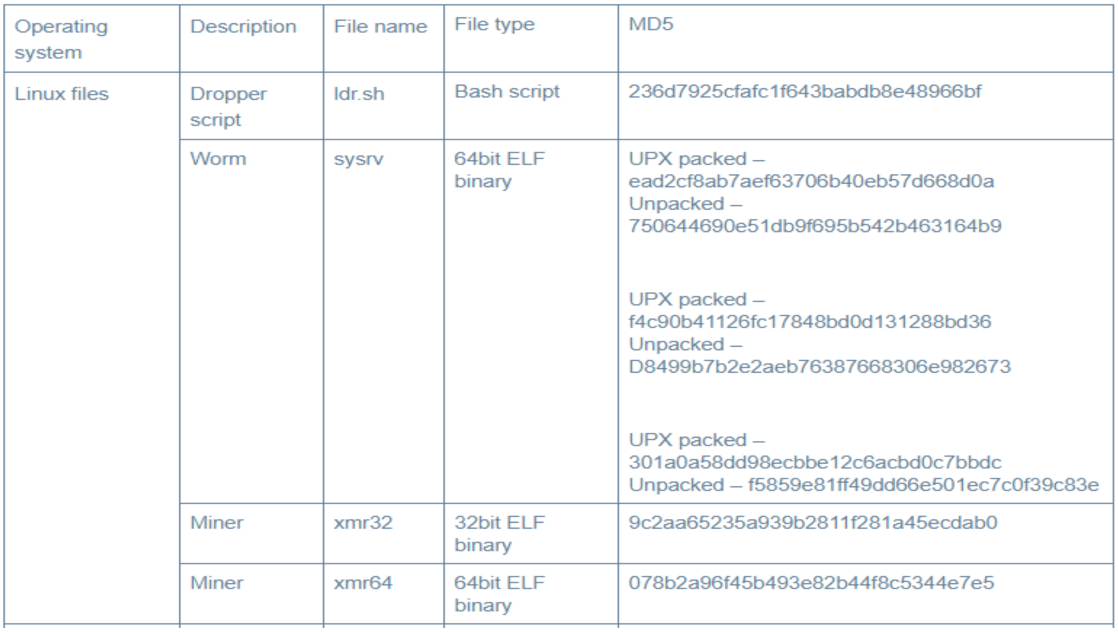
It has been reported that a new Worm is targeting public facing services; **MySQL**, **Tomcat** admin panel and **Jenkins,** having weak passwords, for both **Windows** and **Linux.** The malware also has the ability to maneuver from one platform to the other. The attack uses three files: a Dropper script (bash or powershell), a Golang binary worm, and an XMRig Miner—all of which are hosted on the same C&C.

For further details including technical analysis, please visit following link:
https://www.intezer.com/blog/research/new-golang-worm-drops-xmrig-miner-on-servers/

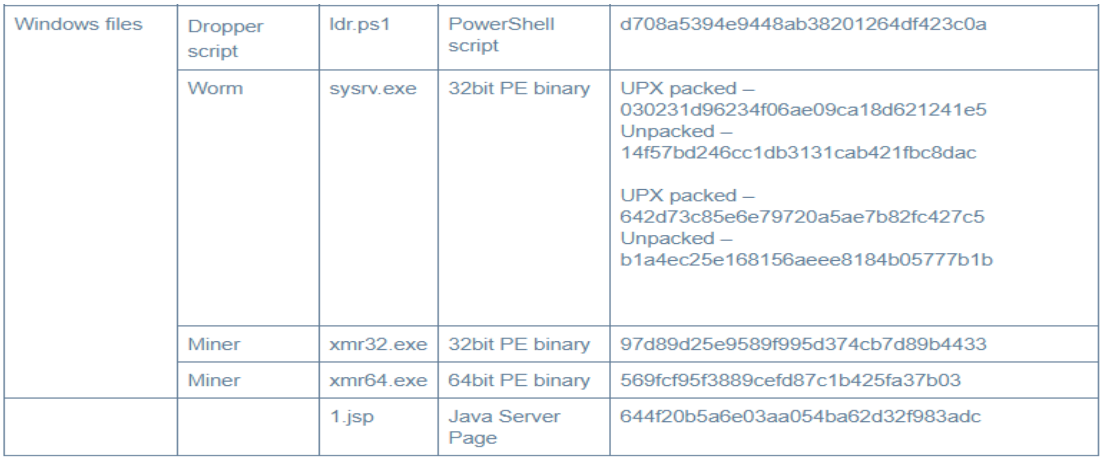
Indicators of Compromise (IoCs):

a. **Command and Control (C&C):** 185.239.242[.]71

b. **Files**



Operating system	Description	File name	File type	MD5
Linux files	Dropper script	ldr.sh	Bash script	236d7925cfafc1f643babdb8e48966bf
	Worm	sysrv	64bit ELF binary	UPX packed – ead2cf8ab7aef63706b40eb57d668d0a Unpacked – 750644690e51db9f695b542b463164b9 UPX packed – f4c90b41126fc17848bd0d131288bd36 Unpacked – D8499b7b2e2aeb76387668306e982673 UPX packed – 301a0a58dd98ecbbe12c6acbd0c7bbdc Unpacked – f5859e81ff49dd66e501ec7c0f39c83e
	Miner	xmr32	32bit ELF binary	9c2aa65235a939b2811f281a45ecdab0
	Miner	xmr64	64bit ELF binary	078b2a96f45b493e82b44f8c5344e7e5



Windows files	Dropper script	ldr.ps1	PowerShell script	d708a5394e9448ab38201264df423c0a
	Worm	sysrv.exe	32bit PE binary	UPX packed – 030231d96234f06ae09ca18d621241e5 Unpacked – 14f57bd246cc1db3131cab421fbc8dac UPX packed – 642d73c85e6e79720a5ae7b82fc427c5 Unpacked – b1a4ec25e168156aeee8184b05777b1b
	Miner	xmr32.exe	32bit PE binary	97d89d25e9589f995d374cb7d89b4433
	Miner	xmr64.exe	64bit PE binary	569fcf95f3889cefd87c1b425fa37b03
		1.jsp	Java Server Page	644f20b5a6e03aa054ba62d32f983adc

Recommendations:

- Always use complex passwords and limit login attempts.
- Always use 2FA (Two-Factor Authentication), wherever possible.
- Update all software including Operating Systems, Servers, etc. to the latest and stable versions with appropriate patches.
- Ensure the principle of least privilege and disable unnecessary services/ ports as malware often exploit such services.
- Install, regularly maintain and update Antivirus solution from a well reputed vendor.
- System Administrators/ Network Administrators to configure host-based firewalls to block outbound connections from Excel.exe, Winword.exe, Wordpad.exe, Mshta.exe, Noptepad.exe, Eqnedt32.exe and ctfmon.exe as Anti-malware solutions alone cannot fully protect against APT attacks.
- Execution of unsigned executables from sensitive webservers and endpoints must be blocked.
- Regularly provide Cyber security awareness sessions for employees and continuously arrange capacity building of the relevant technical resources.
- Do not download attachments from emails unless they are from the trusted source.
- Avoid download/use of cracked and pirated software.
- In case of any incident, please report to this office.