1. Các công cụ được sử dụng để thực hiện rà soát mã độc trên hệ thống Windows

Công cụ kiểm tra mã độc mức nhân hệ điều hành:

STT	Tên công cụ	Các tập tin chạy	Chức năng
1	GMER	GMER.exe	Rà soát, gỡ bỏ mã độc mức nhân hệ điều hành
2	PCHunter	PCHunter32.exe PCHunter64.exe	Rà soát, gỡ bỏ mã độc mức nhân hệ điều hành
3	PowerTool	PowerTool32.exe PowerTool64.exe ShellExtend64.dll	Rà soát, gỡ bỏ mã độc mức nhân hệ điều hành

Công cụ do VCS tự phát triển:

STT	Tên công cụ	Các tập tin chạy	Chức năng
1	CheckInject	CheckInject.exe CheckInjectx64.exe CIGui.exe CIGui64.exe	Kiểm tra, phát hiện mã độc sử dụng kĩ thuật inject code (chèn code độc) vào các tiến trình chuẩn Ghi chú: Công cụ có sử dụng API của Microsoft để check chữ kí số nên sẽ có kết nối mạng ra ngoài đến các địa chỉ máy chủ CA chuẩn của thế giới, các kết nối này là an toàn.
2	QrCode	QrCode+ v2.2.exe	Lấy hash của file, gen thành mã qrcode để tiện cho việc check lên Virustotal
3	SampleCollector	SampleCollector 1.6.exe	Lấy log trong trường hợp cần phân tích mã độc và forensic chuyên sâu. Log bao gồm: file nghi ngờ, timestamp, autoruns, process, network, Windows event log, Windows Prefetch
4	VcsShellScanner	VcsShellScanner32.exe VcsShellScanner64.exe	Quét các file trong thư mục web nhằm kiểm tra, phát hiện webshell
5	RegLastWriteTime	RegLastWriteTime.exe	Trích xuất thông tin thời điểm chỉnh sửa khóa registry
6	RegSwitch	RegSwitch.exe	Công cụ khóa/mở khóa tính năng registry trên windows

Các công cụ trong bộ Sysinternals Suite của Microsoft:

STT	Tên công cụ	Các tập tin chạy	Chức năng
1	Autoruns	Autoruns.exe Autoruns64.dll Autoruns64.exe Autoruns64a.dll autorunsc.exe autorunsc64.exe	Liệt kê các tiến trình được khởi động cùng hệ thống
2	Procexp	procexp.exe procexp64.exe	Liệt kê các tiến trình đang chạy trên hệ thống
3	Procmon	Procmon.exe Procmon64.exe	Monitor hành vi của các tiến trình đang chạy trên hệ thống
4	PsLoggedOn	PsLoggedon.exe PsLoggedon64.exe	Liệt kê danh sách người dùng đang truy cập vào máy tính
5	Handle	handle.exe handle64.exe	Liệt kê handle được mở trong các tiến trình
6	ListDlls	Listdlls.exe Listdlls64.exe	Liệt kê các dll được load trong các tiến trình đang chạy trên hệ thống
7	RegJump	regjump.exe	Truy xuất nhanh đến một khóa registry
8	ProcDump	procdump.exe procdump64.exe	Dump bộ nhớ của tiến trình đang chạy trên hệ thống
9	SigCheck	sigcheck.exe sigcheck64.exe	Hiển thị các thông tin về file: hash, timestamp, chữ kí số…
10	Strings	strings.exe strings64.exe	Trích xuất các xâu ký tự có trong file
11	TcpView	Tcpvcon.exe Tcpview.exe	Liệt kê các tiến trình có các nối mạng với bên ngoài
12	VMMap	vmmap.exe vmmap64.exe	Hiển thị thông tin bộ nhớ của các tiến trình

STT	Tên công cụ	Các tập tin chạy	Chức năng
1	WinRAR	Rar.exe	Nén, mã hóa các tập tin

STT	Tên công cụ	Các tập tin chạy	Chức năng
		rar64.exe	
2	FSum	fsum.exe	Kiểm tra mã hash các tập tin
3	MoveYourMouse	MoveYourMouse.exe	Di chuyển chuột, tránh máy tính bị lock trong quá trình rà soát
4	CFF Explorer	CFF Explorer.exe	Xem thông tin chi tiết một file thực thi
5	JumpListsView	JumpListsView.exe	Xem thông tin JumpLists
6	LastActivityView	LastActivityView.exe	Liệt kê các hoạt động gần đây trên máy tính
7	MFTScan	MFTRCRD.exe MFTRCRD64.exe	Trích xuất thông tin MFT Timestamp của file
8	Notepad++	notepad++.exe	Xem nội dung file txt
9	USBDeview	USBDeview.exe USBDeview64.exe	Xem lịch sử sử dụng USB trên máy tính
10	WinPrefetchView	WinPrefetchView.exe WinPrefetchView64.exe	Xem thông tin prefetch
11	WMIExplorer	WMIExplorer.exe	Xem thông tin các cấu hình WMI trên máy tính

2. Các công cụ được sử dụng để thực hiện rà soát mã độc trên hệ thống Linux

Chỉ sử dụng các công cụ do VCS tự phát triển và các lệnh sẵn có của hệ điều hành.

Công cụ do VCS tự phát triển:

STT	Tên công cụ	Các tập tin chạy	Chức năng
1	VscShellScanner	VscShellScanner_32bit VcsShellScanner_64bit	Quét các file trong thư mục web nhằm kiểm tra, phát hiện webshell.

Các câu lệnh sử dụng trên hệ điều hành Linux:

STT	Câu lệnh sử dụng	Chức năng
1	uname –a	Kiểm tra thông tin của hệ điều hành (SunOS, AIX, Solaris…)
2	ps –auxf ps –aef ps –eo pid,ppid,user,lstart,time,comm,cmd,args –sort=ppid ps –axfo user,pid,ppid,pcpu,pmem,vsz,rss,tname,stat,start,time,args	Thu thập thông tin các tiến trình đang được chạy trên hệ thống
3	hostname	Lấy thông tin tên máy cần rà soát
4	id	Thu thập thông tin những user, group trên hệ thống
5	getenforce	Lấy trạng thái của SElinux mode
6	ip addr show ipconfig –a ip ro show route –n	Thu thập thông tin về IP của hệ thống
7	crontab -l	Thu thập thông tin về crontab của hệ thống
8	systemctl list-timers –all systemctl status *.timers timedatectl	Lấy thời gian hiện tại của hệ thống.
9	ls –latr <folder path>	Thu thập thông tin các file trong folder chỉ định
10	cp	Copy file
11	Printf <string>	In chuỗi ký tự.
12	csum –h <hash type> <File Path> openssl dgst –sha256 <File Path> digest –a <hash type> -v <File Path>	Thu thập file hash của các file

STT	Câu lệnh sử dụng	Chức năng
	md5sum <File Path> sha1sum <File Path> sha256sum <File Path>	
13	find <folder path>	Tìm kiếm file
14	atq	Kiểm tra các job trên hệ thống
15	cat <file path>	Đọc file
16	iptables –L –n –v iptables –t nat –L –n –v ip6tables –L –n –v iptables-save	Lấy thông tin cấu hình iptables
17	netstat -ant netstat –r arp –a lsof –nPi netstat –anop netstat -ntlpuw	Lấy thông tin network của hệ thống
18	stat <file path>	Kiểm tra thông tin cơ bản của file (File size, time, access…)
19	last –a w who –a lastlog	Lấy thông tin về các phiên logon hiện tại
20	chmod +x <File Path> chmod 777 <File Path>	Cấp quyền thực thi cho file
21	dirname	Lấy thông tin parent folder

STT	Câu lệnh sử dụng	Chức năng
22	lsmod modinfo	Hiển thị các modules đang được load trên hệ thống
23	knockd	Command kiểm tra port knock server
24	df –aH	Kiểm tra thông tin của ổ đĩa
25	tar zcf <file compress> <Folder path> tar cvf - <Folder Path> | gzip > <file compress>	Nén các file, folder dữ liệu
26	mv	Di chuyển các file, folder