halcyon | Ransomware Research Center

Crytox Consistently Evades Endpoint Security via PowerShell

The six-year-old Crytox ransomware gang shows signs of actively evolving after many years of maintaining a low profile and relative stagnation. Halcyon observed that the custom built Crytox PowerShell Encryptor is able to evade endpoint detection and response (EDR) and endpoint protection platforms (EPP) without the need for additional tooling, including tools leveraged by multiple other ransomware groups like HRSword.

Crytox targeting continues to focus on virtual infrastructure (hypervisors, VM servers), entry via VPN exploitation, and manual hands-on-keyboard execution, which are all consistent with a deliberate, targeted operation rather than high-volume automated campaigns.

Background:

Crytox is a multi-stage ransomware family first observed in 2020 that has deliberately maintained a low profile relative to its peers. According to publicly confirmed compromises, Crytox early ransom demands were modest. In September 2021, a Dutch broadcasting company publicly confirmed a compromise and paid just 8,500 euros, consistent with a group still in development or intentionally avoiding law enforcement attention.
That changed with a Q1 2025 engagement documented by Cisco Talos, where affiliates exploited a public-facing application lacking multifactor authentication (MFA) to encrypt two hypervisors hosting numerous virtual machine servers. These Q1 2025 engagements also revealed operators using HRSword to disable EDR solutions, a tool not previously publicly associated with Crytox.

By late 2025, Crytox had moved on from HRSWord, developing its own encryptor able to evade EDR and EPP. At the same time, the gang's payloads were being distributed via Shanya, a Packer-as-a-Service sold on underground forums that implements in-memory loading, API hashing, sandbox evasion, and a dual-driver technique to defeat security products.

Crytox modus operandi centers on encrypting files across local disks and network drives with the *.waiting* extension, dropping the uTox messenger application on infected systems for ransom negotiation, and presenting a ransom note with a five-day payment ultimatum. Notably, Crytox does not perform double extortion attacks. The data is encrypted but not exfiltrated, an operational choice less common today. To hinder recovery, an early-stage shellcode component deletes Volume Shadow (VSS) copies and clears event logs before the final encryption payload executes.

Mitigation:

Organizations should adopt layered defenses aligned to common ransomware tactics:

- **Harden Initial Access Vectors:** Reduce exposure from trusted relationships and third-party access pathways [M1030] [M1018].
- **Limit Lateral Movement and Credential Abuse:** Monitor and restrict Remote Services [M1035] [M1032] and misuse of Valid Accounts [M1018] [M1027].
- **Detect Data Staging and Exfiltration:** Monitor for Archive Collected Data [M1047] and Exfiltration Over Command-and-Control Channel [M1031] [M1057].
- **Protect Against Encryption Impact:** Ensure resilience against Data Encrypted for Impact [M1053] through tested recovery processes.
- **Deploy Dedicated Anti-Ransomware Solution:** Deploy dedicated anti-ransomware defenses to block malicious binaries pre-execution [M1038], detect runtime behaviors and data exfiltration attempts [M1040], prevent tampering and network intrusion [M1031], and protect the integrity of backups to reduce extortion leverage [M1053].

Technical Analysis:

Starting in mid-2025, Halcyon investigated an encryption campaign targeting dozens of victims where HRSword was not used for EDR killing. Halcyon determined that software did execute legitimate CryptoAPI calls via the PowerShell script to include CryptGenKey and CryptImportKey. This analysis enabled Halcyon to determine the amount of encryption that occurred in victim environments, and helped victims recover critical data.

Ransomware Payload:

The Crytox ransomware payload is developed in C and typically packed with UPX. It employs a multi-stage shellcode injection into native Windows processes such as explorer.exe and svchost.exe to evade detection. Crytox hinders static analysis through self-decryption across multiple stages, process injection, encrypted configurations, and API hashing.

File encryption uses AES-CBC with a per-file 256-bit key protected by a locally generated RSA keypair, though the use of a weak random number generator with a 32-bit integer seed introduces a known implementation weakness that may allow decryption via brute-force without access to the private key.

- <random-name>.txt (e.g., Raw-text-to-copy-into-PowerShell-Admin-session-and-hit-Enter.txt)
- d3d0bbaf2108ef7cee7ae795e31450135acff39fd95b3ec3af5da9a198d90f97

The crytox_sc.bin.bndb is the extract of the above execution of copying the raw text into a PowerShell Admin session:

- 4ba114ab4f5af6a0457c7e5006617b078796a7af87fe10ffc758e870b326bd44

Process Injection and Termination:

Crytox injects its encryptor payload into legitimate Windows processes to execute encryption under the cover of trusted system binaries. Specifically, it injects encryptor code into explorer.exe and up to two instances of svchost.exe running the netsvcs service.

The encryptor then checks for the existence of an event named YdS, and once triggered, it terminates a list of processes using TerminateProcess. This event is created upon completion of file encryption, and process name hashes are used to identify which processes to terminate. Here is an abbreviated list:

- cmd.exe
- conhost.exe
- csrss.exe
- ctfmon.exe
- dllhost.exe
- dwm.exe
- explorer.exe
- find.exe
- fontdrvhost.exe
- iexplore.exe
- logonui.exe
- lsass.exe
- lsm.exe
- mshta.exe
- mstsc.exe
- notepad.exe
- powershell.exe
- rundll32.exe
- searchindexer.exe
- searchui.exe
- services.exe
- sihost.exe
- smss.exe
- spoolsv.exe
- svchost.exe
- system
- taskhostex.exe
- taskhostw.exe
- taskmgr.exe
- wevtutil.exe
- wininit.exe
- winlogon.exe

Asymmetric Key Generation:

Crytox generates a session RSA key pair to protect per-file encryption keys, ensuring only the attacker can decrypt. The reasons why the keys are needed from the threat actor include the following:

- Generates session RSA-2048 private/public key pair using CryptGenKey.
- Imports RSA-2048 attacker public key (encrypted with single-byte XOR with key 0xcc at offset 0x25e7) using CryptImportKey then encrypts the session private key with it five times, concatenating the results into 0x500 bytes. The encrypted result is also stored in the registry (see Registry Modifications)
- The session public key is used to encrypt the file encryption key info (see below). This public key is also stored in the registry. (see Registry Modifications)

Symmetric Key Generation:

Each file is encrypted with a unique AES-256 key generated at runtime:

- Generates AES-256 file encryption key using CryptGenKey with Algid = CALG_AES_256.
- Used to CryptExportKey to get the raw key bytes generated by CryptGenKey.
- Uses the raw key bytes as the key input to the aes_encrypt function.
- The IV is all zeroes.
- The encryption info is stored in this struct.

struct CipherInfo __packed { BLOBHEADER blob_header; uint32_t key_size; char key[0x20]; uint32_t filesize_hi; uint32_t filesize_lo; uint32_t encrypt_size; int32_t unknown; char unused1[0x44]; };

Registry Modifications:

- Crytox stores its cryptographic material and persistence mechanisms in the Windows registry:
- Adds HKCR\\.wait\\shell\\open\\command registry subkey
  - Adds the following values:
  - “en” = generated RSA session public key
  - “n” = encrypted generated RSA session private key
  - “” = C:\Windows\System32\mshta.exe “C:\Help.hta”

Encryption:

File encryption uses AES-256 in CBC mode, with hardware acceleration via AES-NI when available:

- AES-256 in CBC mode (no padding), either via software or AES-NI depending on the cpu.

Footer Structure:

The following footer is appended at the end of an encrypted file:

Offset	Length	Description
0	0x100 bytes	RSA-2048 encrypted cipher info using generated session public key
0x100	0x500 bytes	RSA-2048 encrypted RSA-2048 session private key using attacker's public key looped 5 times making a total of 0x500 bytes (5 x 100h)

Ransom Note:

- Uses the open command to display the HTA file c:\\Help.hta. This is displayed once file encryption is finished.
- After three reboots, systems were completely unrecoverable showing just a black screen and had to be built from backups or scratch.

Configuration:

Full config starting at offset 0x1c2b. Decrypted using XOR:

Offset	Hex Bytes	ASCII / DECODED
00000000	3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 6d 65 74	<html><head><met
00000010	61 20 63 68 61 72 73 65 74 3d 27 55 54 46 2d 38	a charset='UTF-8
00000020	27 3e 3c 74 69 74 6c 65 3e 52 45 43 4f 56 45 52	'><title>RECOVER
00000030	59 20 54 4f 4f 4c 3c 2f 74 69 74 6c 65 3e 3c 48	Y TOOL</title><H
00000040	54 41 3a 41 50 50 4c 49 43 41 54 49 4f 4e 0d 0a	TA:APPLICATION\r\n
00000050	49 43 4f 4e 3d 27 6d 73 69 65 78 65 63 2e 65 78	ICON='msiexec.ex
00000060	65 27 0d 0a 53 49 4e 47 4c 45 49 4e 53 54 41 4e	e'\r\nSINGLEINSTAN
00000070	43 45 3d 27 79 65 73 27 0d 0a 53 79 73 4d 65 6e	CE='yes'\r\nSysMen
00000080	75 3d 27 6e 6f 27 3e 0d 0a 3c 73 63 72 69 70 74	u='no'>\r\n<script
00000090	3e 77 69 6e 64 6f 77 2e 6d 6f 76 65 54 6f 28 35	>window.moveTo(5
000000a0	30 2c 35 30 29 3b 77 69 6e 64 6f 77 2e 72 65 73	0,50);window.res
000000b0	69 7a 65 54 6f 28 73 63 72 65 65 6e 2e 77 69 64	izeTo(screen.wid
000000c0	74 68 2d 31 30 30 2c 73 63 72 65 65 6e 2e 68 65	th-100,screen.he
000000d0	69 67 68 74 2d 31 30 30 29 3b 3c 2f 73 63 72 69	ight-100);</scri
000000e0	70 74 3e 3c 73 74 79 6c 65 20 74 79 70 65 3d 27	pt><style type='
000000f0	74 65 78 74 2f 63 73 73 27 3e 62 6f 64 79 7b 62	text/css'>body{b
00000100	61 63 6b 67 72 6f 75 6e 64 3a 23 30 30 30 7d 2e	ackground:#000}.
00000110	62 7b 66 6f 6e 74 3a 31 32 30 25 3b 66 6f 6e 74	b{font:120%;font
00000120	2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 63 6f 6c	-weight:bold;col
00000130	6f 72 3a 23 66 66 66 7d 2e 61 7b 62 61 63 6b 67	or:#fff}.a{backg
00000140	72 6f 75 6e 64 3a 23 66 30 30 3b 62 6f 72 64 65	round:#f00;borde
00000150	72 2d 6c 65 66 74 3a 31 30 70 78 7d 2e 71 7b 74	r-left:10px}.q{t
00000160	65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72	ext-align:center
00000170	3b 66 6f 6e 74 3a 32 30 30 25 3b 66 6f 6e 74 2d	;font:200%;font-
00000180	77 65 69 67 68 74 3a 62 6f 6c 64 3b 6d 61 72 67	weight:bold;marg
00000190	69 6e 2d 62 6f 74 74 6f 6d 3a 32 30 70 78 3b 63	in-bottom:20px;c

Offset	Hex Bytes	ASCII / DECODED
000001a0	6f 6c 6f 72 3a 23 66 66 66 7d 3c 2f 73 74 79 6c	olor:#fff}</styl
000001b0	65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 3c	e></head><body><
000001c0	64 69 76 20 63 6c 61 73 73 3d 27 71 27 3e 46 49	div class='q'>FI
000001d0	4c 45 53 20 41 52 45 20 45 4e 43 52 59 50 54 45	LES ARE ENCRYPTE
000001e0	44 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73	D <div clas
000001f0	73 3d 27 62 27 3e 41 6c 6c 20 79 6f 75 72 20 66	s='b'>All your f
00000200	69 6c 65 73 20 77 65 72 65 20 65 6e 63 72 79 70	iles were encryp
00000210	74 65 64 20 61 6e 64 20 69 6d 70 6f 72 74 61 6e	ted and importan
00000220	74 20 64 61 74 61 20 77 61 73 20 63 6f 70 69 65	t data was copie
00000230	64 20 74 6f 20 6f 75 72 20 73 74 6f 72 61 67 65	d to our storage
00000240	3c 2f 62 72 3e 49 66 20 79 6f 75 20 77 61 6e 74	</br>If you want
00000250	20 74 6f 20 72 65 63 6f 76 65 72 20 66 69 6c 65	to recover file
00000260	73 2c 20 63 6f 6e 74 61 63 74 20 74 68 65 20 6f	s, contact the o
00000270	70 65 72 61 74 6f 72 20 69 6e 20 74 68 65 20 54	perator in the T
00000280	4f 58 20 61 70 70 6c 69 63 61 74 69 6f 6e 2c 20	OX application,
00000290	65 6e 74 65 72 20 59 4f 55 52 20 49 44 20 3c 66	enter YOUR ID <f
000002a0	6f 6e 74 20 63 6f 6c 6f 72 3d 4c 69 6d 65 3e 20	ont color=Lime>
000002b0	59 4f 55 52 20 49 44 20 20 3c 2f 66 6f 6e 74 3e	YOUR ID
000002c0	3c 2f 62 72 3e 41 64 64 20 74 68 65 20 49 44 20	</br>Add the ID
000002d0	3c 66 6f 6e 74 20 63 6f 6c 6f 72 3d 42 6c 75 65	<font color=Blue
000002e0	3e 33 43 43 37 43 43 45 46 33 36 39 44 36 41 37	>3CC7CCEF369D6A7
000002f0	41 34 46 36 43 41 44 31 31 44 31 32 44 37 44 45	A4F6CAD11D12D7DE
00000300	36 37 31 39 30 39 39 36 32 39 34 34 41 37 44 30	671909962944A7D0
00000310	33 34 32 38 32 46 31 46 37 42 35 34 46 39 44 33	34282F1F7B54F9D3
00000320	35 32 32 45 35 37 30 32 33 32 41 30 42 3c 2f 66	522E570232A0B</f
00000330	6f 6e 74 3e 20 6f 66 20 79 6f 75 72 20 70 65 72	ont> of your per
00000340	73 6f 6e 61 6c 20 6f 70 65 72 61 74 6f 72 20 61	sonal operator a
00000350	73 20 61 20 66 72 69 65 6e 64 20 73 6f 20 74 68	s a friend so th
00000360	61 74 20 79 6f 75 20 63 61 6e 20 73 74 61 72 74	at you can start
00000370	20 63 68 61 74 74 69 6e 67 2e 3c 2f 62 72 3e 49	chatting.</br>I
00000380	66 20 74 68 65 20 4f 70 65 72 61 74 6f 72 20 64	f the Operator d
00000390	69 64 20 6e 6f 74 20 72 65 73 70 6f 6e 64 20 77	id not respond w
000003a0	69 74 68 69 6e 20 32 34 20 68 6f 75 72 73 20 6f	ithin 24 hours o

Offset	Hex Bytes	ASCII / DECODED
000003b0	72 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 61 6e	r encountered an
000003c0	79 20 70 72 6f 62 6c 65 6d 20 74 68 65 6e 20 73	y problem then s
000003d0	65 6e 64 20 61 6e 20 65 6d 61 69 6c 20 74 6f 20	end an email to
000003e0	6f 75 72 20 73 75 70 70 6f 72 74 20 3c 66 6f 6e	our support <fon
000003f0	74 20 63 6f 6c 6f 72 3d 42 6c 75 65 3e 74 68 61	t color=Blue>tha
00000400	6e 6f 73 73 5f 30 30 31 40 61 6f 6c 2e 63 6f 6d	noss_001@aol.com
00000410	3c 2f 66 6f 6e 74 3e 3c 2f 62 72 3e 49 6e 20 74	</br>In t
00000420	68 65 20 68 65 61 64 65 72 20 6f 66 20 74 68 65	he header of the
00000430	20 6c 65 74 74 65 72 2c 20 69 6e 64 69 63 61 74	letter, indicat
00000440	65 20 79 6f 75 72 20 49 44 20 61 6e 64 20 61 74	e your ID and at
00000450	74 61 63 68 20 32 2d 33 20 69 6e 66 65 63 74 65	tach 2-3 infecte
00000460	64 20 66 69 6c 65 73 20 74 6f 20 67 65 6e 65 72	d files to gener
00000470	61 74 65 20 61 20 70 72 69 76 61 74 65 20 6b 65	ate a private ke
00000480	79 20 61 6e 64 20 63 6f 6d 70 69 6c 65 20 74 68	y and compile th
00000490	65 20 64 65 63 72 79 70 74 6f 72 3c 2f 62 72 3e	e decryptor</br>
000004a0	46 69 6c 65 73 20 73 68 6f 75 6c 64 20 6e 6f 74	Files should not
000004b0	20 68 61 76 65 20 69 6d 70 6f 72 74 61 6e 74 20	have important
000004c0	69 6e 66 6f 72 6d 61 74 69 6f 6e 20 61 6e 64 20	information and
000004d0	73 68 6f 75 6c 64 20 6e 6f 74 20 65 78 63 65 65	should not excee
000004e0	64 20 74 68 65 20 73 69 7a 65 20 6f 66 20 6d 6f	d the size of mo
000004f0	72 65 20 74 68 61 6e 20 35 20 4d 42 3c 2f 62 72	re than 5 MB</br
00000500	3e 41 66 74 65 72 20 72 65 63 65 69 76 69 6e 67	>After receiving
00000510	20 74 68 65 20 72 61 6e 73 6f 6d 2c 20 77 65 20	the ransom, we
00000520	77 69 6c 6c 20 73 65 6e 64 20 61 20 72 65 63 6f	will send a reco
00000530	76 65 72 79 20 74 6f 6f 6c 20 77 69 74 68 20 64	very tool with d
00000540	65 74 61 69 6c 65 64 20 69 6e 73 74 72 75 63 74	etailed instruct
00000550	69 6f 6e 73 20 77 69 74 68 69 6e 20 61 6e 20 68	ions within an h
00000560	6f 75 72 20 61 6e 64 20 64 65 6c 65 74 65 20 79	our and delete y
00000570	6f 75 72 20 66 69 6c 65 73 20 66 72 6f 6d 20 6f	our files from o
00000580	75 72 20 73 74 6f 72 61 67 65 73 3c 2f 64 69 76	ur storages</div
00000590	3e 3c 2f 62 72 3e 3c 64 69 76 20 63 6c 61 73 73	></br><div class
000005a0	3d 27 61 27 3e 3c 64 69 76 20 63 6c 61 73 73 3d	='a'><div class=
000005b0	27 71 27 3e 41 74 74 65 6e 74 69 6f 6e 3c 2f 64	'q'>Attention</d

Offset	Hex Bytes	ASCII / DECODED
000005c0	69 76 3e 3c 75 6c 3e 3c 64 69 76 20 63 6c 61 73	iv> <div clas
000005d0	73 3d 27 62 27 3e 3c 6c 69 3e 44 6f 20 6e 6f 74	s='b'> Do not
000005e0	20 72 65 6e 61 6d 65 20 65 6e 63 72 79 70 74 65	rename encrypte
000005f0	64 20 66 69 6c 65 73 2e 3c 2f 6c 69 3e 3c 6c 69	d files. <li
00000600	3e 44 6f 20 6e 6f 74 20 74 72 79 20 74 6f 20 64	>Do not try to d
00000610	65 63 72 79 70 74 20 79 6f 75 72 20 64 61 74 61	ecrypt your data
00000620	20 75 73 69 6e 67 20 74 68 69 72 64 20 70 61 72	using third par
00000630	74 79 20 73 6f 66 74 77 61 72 65 2c 20 69 74 20	ty software, it
00000640	6d 61 79 20 63 61 75 73 65 20 70 65 72 6d 61 6e	may cause perman
00000650	65 6e 74 20 64 61 74 61 20 6c 6f 73 73 2e 3c 2f	ent data loss.</
00000660	6c 69 3e 3c 6c 69 3e 49 66 20 79 6f 75 20 72 65	li> If you re
00000670	66 75 73 65 20 74 6f 20 70 61 79 20 74 68 65 20	fuse to pay the
00000680	72 61 6e 73 6f 6d 2c 20 49 6d 70 6f 72 74 61 6e	ransom, Importan
00000690	74 20 44 61 74 61 20 74 68 61 74 20 63 6f 6e 74	t Data that cont
000006a0	61 69 6e 73 20 70 65 72 73 6f 6e 61 6c 20 63 6f	ains personal co
000006b0	6e 66 69 64 65 6e 74 69 61 6c 20 69 6e 66 6f 72	nfidential infor
000006c0	6d 61 74 69 6f 6e 20 6f 72 20 74 72 61 64 65 20	mation or trade
000006d0	73 65 63 72 65 74 73 20 77 69 6c 6c 20 62 65 20	secrets will be
000006e0	73 6f 6c 64 20 74 6f 20 74 68 69 72 64 20 70 61	sold to third pa
000006f0	72 74 69 65 73 20 69 6e 74 65 72 65 73 74 65 64	rties interested
00000700	20 69 6e 20 74 68 65 6d 2e 3c 2f 62 72 3e 49 6e	in them.</br>In
00000710	20 61 6e 79 20 63 61 73 65 2c 20 77 65 20 77 69	any case, we wi
00000720	6c 6c 20 72 65 63 65 69 76 65 20 61 20 70 61 79	ll receive a pay
00000730	6d 65 6e 74 2c 20 61 6e 64 20 79 6f 75 72 20 63	ment, and your c
00000740	6f 6d 70 61 6e 79 20 77 69 6c 6c 20 66 61 63 65	ompany will face
00000750	20 70 72 6f 62 6c 65 6d 73 20 69 6e 20 6c 61 77	problems in law
00000760	20 65 6e 66 6f 72 63 65 6d 65 6e 74 20 61 6e 64	enforcement and
00000770	20 6a 75 64 69 63 69 61 6c 20 61 72 65 61 73 2e	judicial areas.
00000780	3c 2f 6c 69 3e 3c 2f 64 69 76 3e 3c 2f 75 6c 3e	
00000790	3c 2f 64 69 76 3e 3c 73 63 72 69 70 74 20 6c 61	<script la
000007a0	6e 67 75 61 67 65 3d 27 56 42 53 63 72 69 70 74	nguage='VBScript
000007b0	27 3e 0d 0a 4f 6e 20 45 72 72 6f 72 20 52 65 73	'>\r\nOn Error Res
000007c0	75 6d 65 20 4e 65 78 74 0d 0a 73 65 74 20 53 3d	ume Next\r\nset S=

Offset	Hex Bytes	ASCII / DECODED
000007d0	43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 57 73	CreateObject(“Ws
000007e0	63 72 69 70 74 2e 73 68 65 6c 6c 22 29 0d 0a 75	cript.shell”)\r\nu
000007f0	74 6f 78 3d 53 2e 45 78 70 61 6e 64 45 6e 76 69	tox=S.ExpandEnvi
00000800	72 6f 6e 6d 65 6e 74 53 74 72 69 6e 67 73 28 22	ronmentStrings(“
00000810	25 77 69 6e 64 69 72 25 5c 75 74 6f 78 2e 65 78	%windir%\utox.ex
00000820	65 22 29 0d 0a 49 66 20 6e 6f 74 20 43 72 65 61	e”)\r\nIf not Crea
00000830	74 65 4f 62 6a 65 63 74 28 22 53 63 72 69 70 74	teObject(“Script
00000840	69 6e 67 2e 46 69 6c 65 53 79 73 74 65 6d 4f 62	ing.FileSystemOb
00000850	6a 65 63 74 22 29 2e 46 69 6c 65 45 78 69 73 74	ject”).FileExist
00000860	73 28 75 74 6f 78 29 20 54 68 65 6e 0d 0a 4d 73	s(utox) Then\r\nMs
00000870	67 42 6f 78 20 22 46 69 6e 64 20 61 6e 64 20 64	gBox “Find and d
00000880	6f 77 6e 6c 6f 61 64 20 55 54 4f 58 2e 45 58 45	ownload UTOX.EXE
00000890	20 66 69 6c 65 20 6f 6e 20 74 68 65 20 49 6e 74	file on the Int
000008a0	65 72 6e 65 74 20 61 6e 64 20 73 74 61 72 74 2e	ernet and start.
000008b0	2e 2e 22 0d 0a 45 6e 64 20 49 66 0d 0a 53 2e 52	..”\r\nEnd If\r\nS.R
000008c0	75 6e 20 75 74 6f 78 20 26 20 22 20 2d 70 22 2c	un utox & “ - p”,
000008d0	31 0d 0a 3c 2f 73 63 72 69 70 74 3e 3c 2f 62 6f	1\r\n</script></bo
000008e0	64 79 3e 3c 2f 68 74 6d 6c 3e 77 00 69 00 6e 00	dy></html> [UTF-16: w.i.n.]
000008f0	64 00 6f 00 77 00 73 00 00 00 48 00 65 00 6c 00	[UTF-16: d.o.w.s.] \0\0 [UTF-16: H.e.l.]
00000900	70 00 2e 00 68 00 74 00 61 00 00 00 5c 00 5c 00	[UTF-16: p..h.t.a.] \0\0 \\.\\.
00000910	3f 00 5c 00 43 00 3a 00 5c 00 2a 00 2e 00 2a 00	[UTF-16: ?.\.C.:.\.*..*.]
00000920	00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00	\0\0 space \0 padding
00000930	00 00 00 00 00 00 2e 00 77 00 61 00 69 00 74 00	padding [UTF-16: ..w.a.i.t.]
00000940	00 00 63 3a 5c 77 69 6e 64 6f 77 73 5c 73 79 73	\0\0 c:\windows\sys
00000950	74 65 6d 33 32 5c 6d 73 68 74 61 2e 65 78 65 20	tem32\mshta.exe
00000960	22 63 3a 5c 68 65 6c 70 2e 68 74 61 22 00 2e 77	“c:\help.hta”\0 .w
00000970	61 69 74 5c 73 68 65 6c 6c 5c 6f 70 65 6e 5c 63	ait\shell\open\c
00000980	6f 6d 6d 61 6e 64 5c 00 6f 70 65 6e 00 53 4f 46	ommand\ open SOF
00000990	54 57 41 52 45 5c 4d 69 63 72 6f 73 6f 66 74 5c	TWARE\Microsoft\
000009a0	57 69 6e 64 6f 77 73 5c 43 75 72 72 65 6e 74 56	Windows\CurrentV
000009b0	65 72 73 69 6f 6e 5c 52 75 6e 5c 00 06 02 00 00	ersion\Run\ \0 06 02 00 00
000009c0	00 a4 00 00 52 53 41 31 00 08 00 00 01 00 01 00	\0 a4 \0\0 RSA1 [keylen=0x800] [pubexp=0x10001]

Offset	Hex Bytes	ASCII / DECODED
000009d0	f5 fa 04 10 9b 4d 44 bd cf 89 e6 2d 89 62 81 38	[RSA modulus bytes 0x00-0x0F]
000009e0	80 28 75 41 29 c3 05 b7 84 23 89 5b 55 b4 ba e5	[RSA modulus bytes 0x10-0x1F]
000009f0	42 8f 54 da 73 f5 4f 3a 5d 3e d0 7c c5 ea 33 82	[RSA modulus bytes 0x20-0x2F]
00000a00	f7 8e 2b f2 b8 b2 89 01 ea fc 87 b3 63 70 fd 76	[RSA modulus bytes 0x30-0x3F]
00000a10	6b bb 86 57 f2 e6 86 4b 38 f6 a7 84 7a 76 20 a7	[RSA modulus bytes 0x40-0x4F]
00000a20	4c 26 fa 11 7d 4f e6 f5 45 76 f3 a7 1e 61 45 df	[RSA modulus bytes 0x50-0x5F]
00000a30	5e e8 b5 41 9e b5 85 4f 1e 6a 4d eb 2f 29 29 df	[RSA modulus bytes 0x60-0x6F]
00000a40	40 9d a8 51 b0 b6 e7 d0 11 79 74 f0 38 99 5c e5	[RSA modulus bytes 0x70-0x7F]
00000a50	fd f2 b8 e7 18 66 b1 b7 17 73 8f 85 f8 41 93 ae	[RSA modulus bytes 0x80-0x8F]
00000a60	7a 19 61 1a 6a 7b ad 48 fb c5 99 d2 60 79 40 21	[RSA modulus bytes 0x90-0x9F]
00000a70	d5 c3 d5 ca 4e 92 2f d6 76 39 21 97 ae 2a 8c 1d	[RSA modulus bytes 0xA0-0xAF]
00000a80	2d 6f f4 02 6c 13 19 55 e4 3d b9 e4 31 04 5c c3	[RSA modulus bytes 0xB0-0xBF]
00000a90	be 88 94 42 b3 68 81 cd 4c c9 83 17 08 dd 4e 4e	[RSA modulus bytes 0xC0-0xCF]
00000aa0	e9 b6 2f 2a 0e 74 7f f1 3a 2b 8d e2 7a 13 bd a5	[RSA modulus bytes 0xD0-0xDF]
00000ab0	8a fc 2a 2a 92 5f 50 8f d4 ed 35 de d9 43 4f be	[RSA modulus bytes 0xE0-0xEF]
00000ac0	22 52 35 ca 4d d7 36 bd b1 01 2e 3e 4d d2 69 b3	[RSA modulus bytes 0xF0-0xFF] (truncated)

Conclusion:

Crytox represents a threat actor that has quietly matured over six years into a capable and operationally disciplined ransomware group. Its ability to evade EDR and EPP solutions natively via PowerShell, without reliance on external tooling like HRSword, marks a meaningful tactical evolution and signals that the group is actively adapting its tradecraft to defeat modern defenses. Organizations operating virtual infrastructure and VPN-dependent environments should treat Crytox as a credible and persistent threat and ensure that detection capabilities extend beyond signature-based approaches to cover the behavioral patterns and living-off-the-land techniques this group increasingly relies upon.

The Halcyon Ransomware Research Center unites experts, drives smart policies, and delivers actionable intelligence to detect, disrupt, and defeat ransomware. Explore the Center's latest reports, analysis, and resources here.