Italian VIRUS Magazine

LA PRIMA RIVISTA ITALIANA DEDICATA ALLA LOTTA ANTI-VIRALE MS-DOS

N. 3 - Gennaio - Giugno 1996

Italian VIRUS Magazine

Italian VIRUS Magazine è una rivista elettronica dedicata alla lotta antivirale con particolare attenzione alla realtà italiana, con l'obiettivo di sensibilizzare la comunità informatica verso gli agenti patogeni che ogni giorno tentano di insidiare i nostri calcolatori e quindi il nostro prezioso lavoro.

I.V.M. (Italian VIRUS Magazine) è gratuita, quindi liberamente copiabile e distribuibile senza scopo di lucro.

Uso delle informazioni contenute in I.V.M.

Hanno collaborato:

Gianfranco Tonello, Enrico Tonello, Federico Pellegrin

Via Sardegna n° 5
35030 Sarmeola di Rubano (PD)
Tel./Fax 049-631748 (Fax 24h/24)

NEWS

di Enrico Tonello

13 Maggio: Nuovo Virus MOLOCH

Virus residente in memoria, stealth, polimorfico, crittografato, infetta il Master Boot Record del disco fisso e il boot sector dei floppy. Il polimorfismo utilizzato dal virus Moloch è similare a quello generato dal codice virale Lilith. Il virus Moloch contiene al suo interno il seguente testo:

OH-MY GOD!
Moloch (tm) is here!
Moloch is a trademark of SquiBoyz

Il virus Moloch viene intercettato da VirIT Lite v. 1.04.

27 Aprile: Situazione sui generatori di virus

Attualmente sono stati ritrovati i seguenti generatori di virus:

VCS Virus Construction Set
VCL Virus Creation Laboratory
PS-MPC Phalcon/Skism Mass-Produced Code Generator
G2 The Second Generator
NRLG Nuke Randomic Life Generator
IVP Istant Virus Production
VC2000 Virus Creation 2000

VCS: Virus Construction Set
Gruppo:
Autore:
Note: Crea codici virali lunghi 1077 bytes, individuabili con un'unica stringa;

VCL: Virus Creation Laboratory 1.00
Gruppo: Nuke
Autore: NoWhere Man
Note: Infetta solo COM ad azione diretta, sovrascrittura COM/EXE e cavalli di troia;

PS-MPC: Phalcon/Skism Mass-Produced Code Generator 0.90 beta

Gruppo: Phalcon/Skism
Autore: Dark Angel
Note: 150 routine di crittografazione, infetta COM/EXE, COMMND.COM;

G2: The Second Generator in Virus Creation 0.70 beta
Gruppo: Phalcon/Skism
Autore: Dark Angel
Note: infezione COM/EXE, residente e non, semi-polimorfismo;

NRLG: Nuke Randomic Life Generator v. 066 beta
Gruppo: Nuke - Warez
Autore: Azrael
Note: infetta solo COM, residente e utilizza routine di crittografazione;

IVP: Istant Virus Production Kit v. 1.0
Gruppo: YAM - Youngsters Against McAfee
Autore: Admiral Bailey
Note: infezione COM/EXE, cavalli di troia, infezione COMMAND.COM e opzione di sovrascrittura;

VC2000: Virus Creation 2000 - The Virus Construction Kit
Gruppo: Havoc The Chaos
Autore: John Burnette
Note: infezione COM/EXE/BIN/OVL/SYS/BAT/VXD/DLL, sovrascittura e azione diretta;

26 Aprile: Virus MURUROA

Il virus è stato scoperto nel mese di Marzo 1996 dal ricercatore Gianfranco Tonello. Il codice virale Mururoa è residente in memoria, crittografato, stealth e infetta i files con estensione .COM e .EXE. Il codice virale è lungo 2464 bytes, al suo interno sono visibili le segueti stringhe:

I have one mesage to all people on earth:

Stop all French nuclear testing in the PACIFIC
Dont forgot :Comon peolple dont like nuc. tests!
This is is a MURUROA 1.386 by Blesk

PLUTONIUM IS BETTER IN POWER-PLANT !!!!!

My greet to VYVOJAR,SVL,METABOLIS and all IRC.

Inoltre contiene il nome di quasi tutti gli antivirus.

20 Aprile: Infezioni nel mese di Marzo 1996

Anche in questo mese vi sono state infezioni di virus, non si sono registrate novità significative.

Segnaliamo le seguenti infezioni: HLLC.Crawen.8306, Bye, Form, RPS2, B1, Junkie.1027, Boot.446, AntiExe, Invisible_Man.2926, Parity_Boot.B, Run_Error.505D:5658, Italy, November_17th.900.C, November_17th.855, One_Half.3544, Beethoven, Tequila, Anticmos, Cascade.1701.New, Paris e Barrotes.1310.

09 Aprile: Nuovo virus ELI

I ricercatori della TG Soft stanno analizzando un nuovo virus ritrovato attivo nel sud Italia. Il codice virale è residente in memoria e crittografato ed infetta i file con estensione .COM. All'interno il virus contiene il seguente testo:

SLEEP AND DANCE WITH THE DEATH ELI IS HERE!

Ooops...I deletede your file!..Be happy and don't cry!..
ELI (C) METAL MANIA

Il virus è pericoloso perchè è in grado di sovrascrivere i dati del disco fisso (quindi può danneggiare le informazioni in esso contenute).

14 Marzo: BOZA/BIZATCH viru per WIN 95

Questo codice virale è stato il primo virus scritto per il sistema operativo Windows 95. Facciamo notare che non risulta essere circolante, ne in Italia ne all'estero!
Il virus è stato denominato con il nome di BOZA, ma il suo VERO NOME è BIZATCH come afferma lo stesso autore che lo ha distribuito attraverso il sesto

numero della rivista VLAD. L'autore, l'australiano Quantum, è inoltre stretto collaboratore della rivista. Riportiamo il testo contenuto dal virus BOZA (se cosi' si puo' chiamarlo):

The taste of fame just got tastier!
VLAD Australia does it again with the world's first Win95 Virus.
From the old school to the new.
Metabolis
Qark
Darkman
Automag
Antigen
RhinceWind
Quantum
Absolute Overload
CoKe
Please note the name of this virus is [Bizatch] written by Quantum of Vlad

Bizatch by Quantum / VLAD.

Come si può notare, il nome dato al codice virale dall'autore è molto chiaro, e la stringa BOZA non risulta all'interno del codice virale. Siccome il codice virale è stato distribuito attraverso una rivista elettronica di virus-writer non puo' essere considerato circolante o attivo. Se ogni produttore di anti-virus, chiama lo stesso codice virale con nomi diversi, si crea solo confusione e danno agli utenti.

13 Marzo: Emilia Romagna colpita da B1

Il virus citato, noto anche come NYB, Š stato segnalato molto attivo in Emilia Romagna, ed in particolar modo nelle provincie di Modena e Ferrara. Per il suo corretto risconoscimento è disponibile in area file l'ultima versione di VirIT Lite

11 Marzo: Virus Run_Error.504d:5658

Il virus citato e' diffuso oramai in tutta Italia, numerose segnalazioni sono giunte dal Nord (in particolare da Cremona e Milano), dal centro (Latina, Firenze e Roma) e dal sud. Il virus viene segnalato anche da antivirus che

aderiscono allo standard americano N.C.S.A. con il nome di Peter_II.RunTime. Si tratta di un virus extra traccia nei floppy disk e viene correttamente identificato dall'ultima versione di VirIT Lite.

14 Febbraio: Nuovo virus dalla Polonia

Il ricercatore antivirus Luigi Origa, ha avuto modo di intercettare un nuovo codice virale proveniente dalla Polonia, e arrivato in Italia attraverso un messaggio di posta elettronica della rete packet radio amatoriale agganciato ad un file uuencodato che contiene il file TXT2COM.COM.
Questo file è stato infettato dal Gdynia e successivamente compressato con il programma PKlite. Il virus è stato catalogato dagli analisti della TG Soft con il nome Gdynia (da una stringa contenuta all'interno del codice virale). Gdynia è una città polacca che si affaccia sul mar Baltico. L'ultima versione di VirIT Lite identifica correttamente questo codice virale.

Generatori di codici virali

di Federico Pellegrin

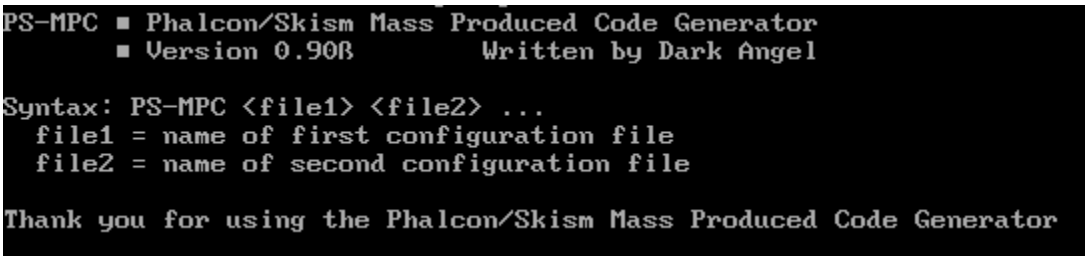
Negli ultimi anni la quantita' di virus in circolazione ha subito una grande impennata grazie alla continua espansione dei gruppi di virus writer.
A questi pero', aprofittando della moltitudine di sorgenti che gli ormai famosi gruppi distribuivano per invogliare i neoprogrammatori a scegliere l'oscuro ma tanto intrigante mondo del virus writing, si e' aggiunta anche una folta schiera di programmatori di codice virale meno esperti. A dare man forte a questi criminali casalinghi, che all'inizio forse avevano solo l'intenzione di fare uno scherzo o di vendicarsi dell'amico, ecco i generatori di codice virale, ovvero dei programmi che creano dei virus vivi, pronti a commettere atti illeciti. Anche qui, come nello scrivere virus, e' nata una vera e propria gara tra i vari gruppi.
Il primo di questi generatori fu il VCS in grado di creare dei virus sovrascriventi. Le sue creazioni
pero' furono molto barbare e presto le sue creazioni vennero debellate.
In sequito ci fu il primo generatore dei NuKE: il VCL. Questo ebbe molto piu' succeso nonostante la semplicita' dei virus che esso generava. Basta pensare al grande numero di virus e varianti di tipo VCL che si trovano nel mondo informatico. Ben presto pero' venne la risposta dei Phalcon/Skism con il loro PS-MPC (Phalcon/Skism Mass-Produced Code Generator) scritto dal ormai famoso Dark Angel. Non molto piu' tardi i PS crearono un'altro generatore di codice virale: il Gý. Anche se il creatore di questo programma, Dark Angel, rinnega di aver solo migliorato il precedente PS-MPC sono riscontrabili molte ugualianze tra i codici generati dai due programmi e potremmo quasi dire che l'ultimo e' solo un miglioramento del primo.
Nel frattempo anche i YAM (Youngsters Against McAfee) diedero un suo

contributo con l' IVP (Instant Virus Production Kit) che ebbe una mediocre espansione dovuta anche questa volta allo scarso rendimento del codice.
Alla fine e' arrivato ancora il prodotto dei NuKE con il NRLG, molto piu' avanzato in certi aspetti, ma che per fortuna per adesso non ha avuto uno gran sviluppo tra i PC nel mondo. Di generatori di codice virale ce ne sono molti in giro (ad esempio non ho citato il VC2000 recensito nel numero precedente) ma purtroppo sono ancora all'oscuro delle conoscenze dei ricercatori antivirus e percio' sono delle vere e proprie mine vaganti.
Ma adesso cerchiamo di esaminare meglio dal lato tecnico e soprattutto valutiamo un po' il pericolo di ognuno di questi generatori:

- **PS-MPC (Phalcon/Skism Mass-Produced Code Generator)**
- **G2 (The Second Generation in Virus Creation)**
- **IVP (Instant Virus Production kit)**
- **NRLG (NuKE Randomic Life Generator)**

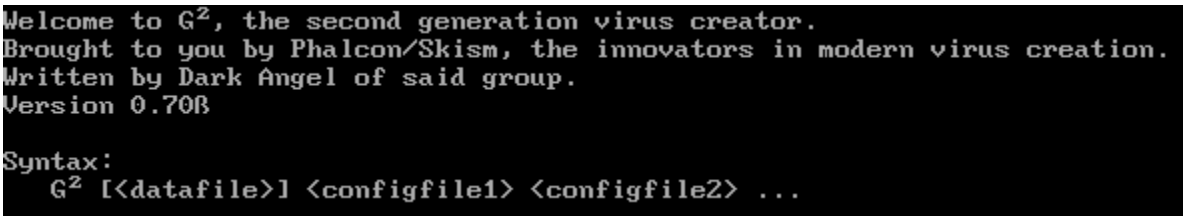
PS-MPC (Phalcon/Skism Mass-Produced Code Generator)

Questo programma crea il codice virale desiderato in base a delle opzioni che vengono scritte in un file dall'utente. Il codice virale creato dal PS-MPC puo' infettare i files eseguibili di tipo COM o di tipo EXE o anche se desiderato ambeddue. Il virus che viene creato non e' residente e puo' essere configurato in modo che infetti tutti o solo un dato numero di files per non dare troppo nell'occhio facendo rallentare troppo il sistema.
Per quanto riguarda l'infezione l'utente puo' specificare se il prodotto infettera solo i files nella directory nella quale viene eseguito il programma infetto o se utilizzera' la 'Dot-Dot method', ovvero, nel caso che il numero di files infetti non sia ancora sufficente, esso tentera' di tramandare l'infezione nella directory precedente. In piu' le creazioni del PS-MPC possono essere anche encrittate con un semplice XOR di words oppure con una somma e relativa sottrazione nel momento della decrittazione. Il generatore di codice virale dei PS inoltre ha la possibilita' di negare messaggi di errore mascherando l'interrupt 24h. Il codice virale creato dal PS-MPC non contiene routine pericolose che possano danneggiare il sistema, ma ha solo lo scopo di moltiplicarsi.



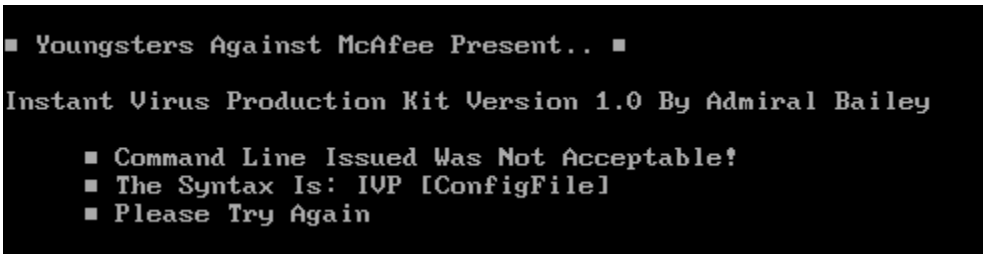
G2 (The Second Generation in Virus Creation)

Quest'altro programma dei PS e' piu' avanzato rispetto al primo. Questo generatore di codice virale infatti ha la possibilita' di creare anche virus residenti in memoria. Inoltre il G2 puo' creare da un unico file di configurazione molti virus diversi: infatti esso contiene una routine che modifica leggermente il codice cosicche' la classica ricerca di virus usando una stringa diventa inusabile. Del resto invece il codice virale e' molto simile alle creazioni del PS-MPC. Infatti gran parte delle creazioni del G2 sono riconosciute dai piu' noti pacchetti antivirus come nuove varianti del PS-MPC.

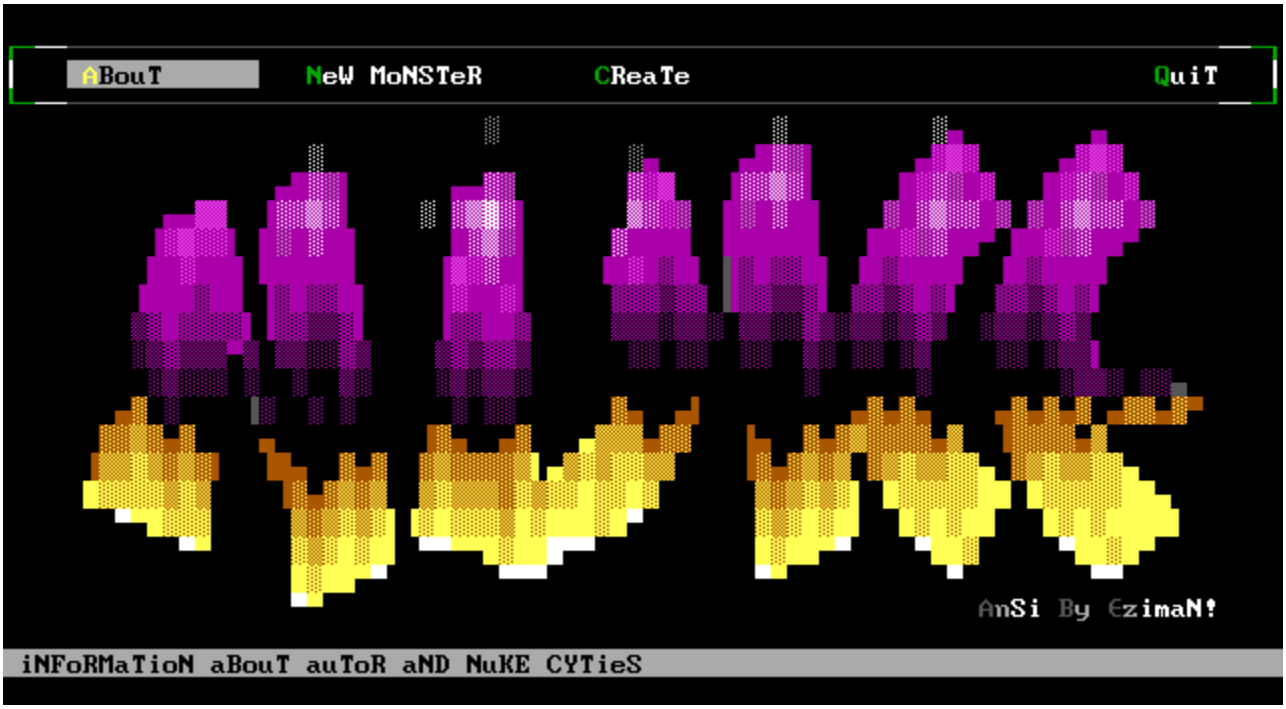


IVP (Instant Virus Production kit)

L'IVP dell' Admiral Bailey ha molte similitudini al primo generatore da me descritto. Infatti come il PS-MPC l'IVP puo' creare solo virus non residenti e puo' appendere il proprio codice alla fine delle vittime. Oltre a questo l'IVP puo' creare anche virus sovvrascriventi, che pero' per il loro barbarico modo di espandersi sono senz'altro preda facile per gli antivirus. Nonostante le creazioni dell'IVP siano molto semplici e non siano in elevato numero, l'IVP a mio parere e' uno dei generatori di codice virale piu' pericoloso tra gli altri qui descritti. Infatti, proprio per i pochi prodotti da esso creati, il codice virale che l'IVP produce puo' essere facilmente modificabile mascherando assolutamente la presenza di un virus. Questo perche' dai primi due generatori di codice virale sono state fatte molte varianti (oltre il centinaio) e percio' gli antivirus non si basano piu' sulla semplice ricerca di una stringa, ma cercano di trovare un certo numero di corrispondenze per potersi accertare dei generatori dei PS.



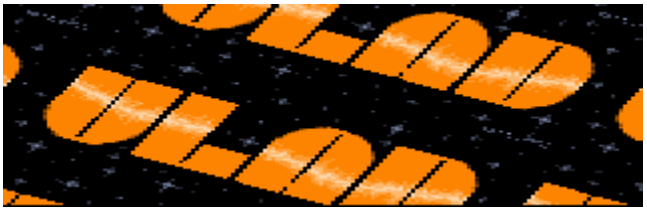
NRLG (NuKE Randomic Life Generator)



Questo generatore e' stato scritto da Azrael (membro dei NuKE). Come in tutte le creazioni dei NuKE ci sono molte schermate ANSI e scritte cubitali raffiguranti il loro stemma. Il NRLG e' (secondo la mia conoscenza) il piu' avanzato generatore di codice virale in circolazione. Comunque esso non e' il piu' pericoloso, dato che il codice virale da esso creato non e' del tutto funzionante e per rimetterlo in sesto ci vuole una mano esperta e dunque la pericolosita' di questo strumento non e' eccessiva. Torniamo adesso alle potenzialita' del NRLG: esso crea virus residenti in grado di infettare solo i files eseguibili di tipo COM. I prodotti del NRLG pero' hanno uno schema di encrittazione piu' complesso scelto casualmente ad ogni generazione ed e' questa la principale potenzialita' di questo generatore. I virus possiedono uno schema di encrittazione composto da molti comandi semplici (inc, dec, not, add, sub) che pero' messi insieme possono significare una buona difesa. Inoltre il codice virale prodotto dal NRLG ha utilizza dei trucchi per sgominare la maggior parte dei software antivirus (residenti in memoria e non). Il NRLG (come dal resto il VCL) puo' compiere determinate azioni in certe date, tra le quali anche alcune veramente molto pericolose, quali cancellare un dato numero di settori o attivare una bomba da MBR.

VLAD Magazine #5

di Federico Pellegrin



Dopo una lunga attesa tra i virus writer e' uscito il quinto numero della rivista del gruppo australiano VLAD, nel quale troviamo molti articoli sui virus e alcuni sorgenti di questi. In questo numero i riflettori sono pero' puntati su due parti molto importanti nella creazione di virus: il polimorfismo e la infezione di programmi che girano sotto Windows. Tutti gli articoli possono esser letti con un semplice editor o sfogliati tramite l'apposito programma che offre dei menu a tendina per consultare gli articoli e le sorgenti virali in un modo piu' colorito. Notevole e' anche l'effetto grafico (comunque gia' visto molte volte nei vari demo grafici) che viene effetuato prima della comparsa del menu (si vedono roteare varie scritte 'VLAD' in modo abbastanza carino). Ma veniamo alla rivista vera e propria analizzando ogni menu a tendina e i suoi contenuti:

EDITORIAL

In questo spazio Metabolis (componente dei VLAD che scrive questa rivista) descrive la situazione del gruppo ed espone dove trovare e come usare questa rivista. Come di solito poi viene menzionata la 'Secret Area', ovvero una porzione ritenuta di grande importanza e percio' per accedervi ci vuole una parola d'ordine. In questo numero oltre alla parola segreta per entrare nell'area segreta si deve anche vincere una partita al gioco del 'Campo minato'. A questo punto verra esposto al lettore la sorgente del virus Myddraal scritto dal virus writer Neuron. Il Myddraal e' un boot infector che pero' (questo viene anche esplicitamente detto all'inizio) non e' del tutto funzionante.

ARTICLES

In questo spazio ci sono due articoli interessanti che descrivono la storia e la situazione attuale di due gruppi di virus writer molto conosciuti nel mondo informatico. I primi sono gli AIH (Australian Institute of Hackers) molto noti in passato per i virus della serie Australian_Parasite (si conta che ce ne siano circa 50 in giro). Il secondo gruppo descritto invece sono gli Immortal Riot, gruppo svedese noto per la pubblicazione della rivista Insane Reality ed anche per aver scritto molti virus (tra i quali citiamo i famosi Scitzo e Manzon). Le due storie sono abbastanza interessanti e descrivono i due gruppi dall' inizio della loro attivita' ad oggi (per gli AIH la carriera e' finita gia' molto tempo fa per delle incomprensioni tra i vari componenti). Nello spazio 'Articles' poi ci sono le sorgenti di due virus che ormai hanno gia' fatto storia, due virus tristemente molto famosi nel popolo informatico: il Neuroquilla e l' Uruguay#3. Infine in questo menu troviamo anche la sorgente di una variante dell' Australian_Parasite e la sorgente con la documentazione completa di un nuovo motore polimorfo: il FOG (the Funky Opcode Generator). Questo motore non e' al momento riconosciuto dai maggiori software antivirus anche se certe mutazioni dei virus che al momento usano FOG (AirRaid) insospettiscono gli antivirus euristici.

MISC

Nel menu centrale della rivista troviamo un interessante documento sulle chiamate alle API di Windows in assembler. Dopodiche' possiamo vedere ben tre motori polimorfici: il Poly Primer, il NoMut (Noone Mutation Engine) 0.01 e il SDFE (Super Deformed Engine) e2.0. Tutti e tre vengono forniti con relative istruzioni d'uso e con una sommaria descrizione del motore. Questi motori polimorfi possono risultare molto pericolosi dato che nessun antivirus rileva neanche minimamente la loro presenza. Inoltre nel menu 'Misc' troviamo anche le sorgenti di due virus polimorfi: il Demon3b ed il Zhuhe Liang v2. Il primo, un COM/EXE infector con elevate capacita' di nascondersi, non viene ancora riconosciuto o euristicamente individuato da nessun antivirus, mentre il secondo, anche esso un COM/EXE infector meno complesso pero' del Demon3b, viene individuato come file sospetto.

VIRUSES - SCRIPTS

Questa volta riuniamo questi due menu, dato che in ambeddue troviamo sorgenti di virus. In questi due spazi troviamo ben 12 sorgenti di virus ed inoltre un piccolo esempio di come sostituire il vecchio interrupt con l'interrupt handler del virus in modo che gli antivirus residenti in memoria piu' avanzati non lo trovino. Vediamo adesso brevemente i virus:

Horsa:	virus non residente che infetta i files .COM. Interessante solo per la strana tecnica utilizzata per infettare i files.
Ph33r:	virus residente che infetta i .COM, gli .EXE e anche gli eseguibili di Windows.
Wintiny:	virus non residente che infetta gli eseguibili di Windows.
Midnight:	virus residente in memoria che infetta i files .COM. Il virus puo' risultare difficile da cancellare, dato che la vittima viene encrittata completamente.
Arme Stoevlar:	virus residente che infetta i files .COM.
Small virus:	virus residente che infetta gli eseguibili .COM e .EXE. E' notevole la lunghezza del virus che e' di soli 168 bytes.
Alive:	un interessante virus residente con elevate capacita' di nascondere la propria presenza in memoria e sul disco.
WinLamer2:	un altro virus che infetta i files di Windows. E' notevole l'uso del motore polimorfo PMEW (il motore in precedenza fu usato anche sotto DOS con il nome di PME).
Lady Death:	virus residente che infetta i .COM e gli .EXE con capacita' di sconfiggere alcuni antivirus TSR.
H8YourNME's:	virus residente che infetta i .COM con alcune possibilita' di nascondersi.
SepBoot:	virus residente che infetta la MBR ed il boot sector con implementate alcune tecniche di stealth.
Fame:	virus residente che infetta i .COM, gli .EXE e il boot sector.

Inoltre insieme alla rivista viene fornito un .ZIP contenente tutti i virus descritti nella rivista gia' compilati e pronti per sprigionare pericolose epidemie virali.

Analisi Virus

coordinatore Gianfranco Tonello

- Barrotes.1310
- Boot.388
- DelCMOS.B

Barrotes.1310

di Gianfranco Tonello

Nome virus:	Barrotes.1310
Aliases:	
Variante:	
Stato:	Comune
Isolato:	Fine 1992
Sintomi:	diminuzione della memoria libera del sistema
Origine:	Spagna
Dimensione:	1310 bytes
Tipo:	Residente in memoria, infetta files .COM e .EXE
Analisi a cura di:	Gianfranco Tonello (e-mail: tge@maya.dei.unipd.it)

COMMENTO GENERALE

Questo codice virale è noto dalla fine del 1992 e la sua provenienza è sicuramente spagnola. Il virus è residente in memoria (TSR), non crittografato ed infetta i file
con estensione .EXE e .COM. Quando un programma infetto dal Barrotes.1310 viene eseguito il virus si installa in memoria allocando 1600 bytes ed intercetta gli interrupts 21H (funzioni DOS) e 24H (gestione degli errori critici) e il 5 gennaio anche l'interrupt 1CH (User Timer Tick) e infetta il COMMAND.COM posto in radice.
Ogni file eseguito con estensione .EXE e .COM (con lunghezza compresa tra 256
e 64002 bytes) verrà infettato, la lunghezza dei file colpiti aumenterà di 1310 bytes. I files infetti sono marcati alla fine con la stringa SO. La data e l'ora dei files infetti non vengono alterate.
Il virus si attiva il 5 gennaio sovrascrivendo il master boot record (MBR) del disco fisso con i primi 512 bytes del codice virale, con la conseguenza che non si può accedere al disco fisso. In questa data viene intercettato l'interrupt 1CH (User Timer Tick), il quale visualizza a video in alto a sinistra il seguente messaggio:

Virus BARROTES por OSoft

di colore bianco su sfondo blu, inoltre vengono visualizzate 8 colonne di vario colore, composte dai caratteri °±² che prendono tutto lo schermo.
Il messaggio visualizzato a video risulta essere crittografato. Il codice virale

Barrotes contiene inoltre la stringa c:\command.com che risulta essere visibile, cioè non crittografata.
Esistono altre due varianti del virus Barrotes, lunghe rispettivamente 1194 e 1303 bytes. Il virus Barrotes.1303 risulta essere crittografato e contiene inoltre il seguente testo:

Sta Tecla (MAD1)

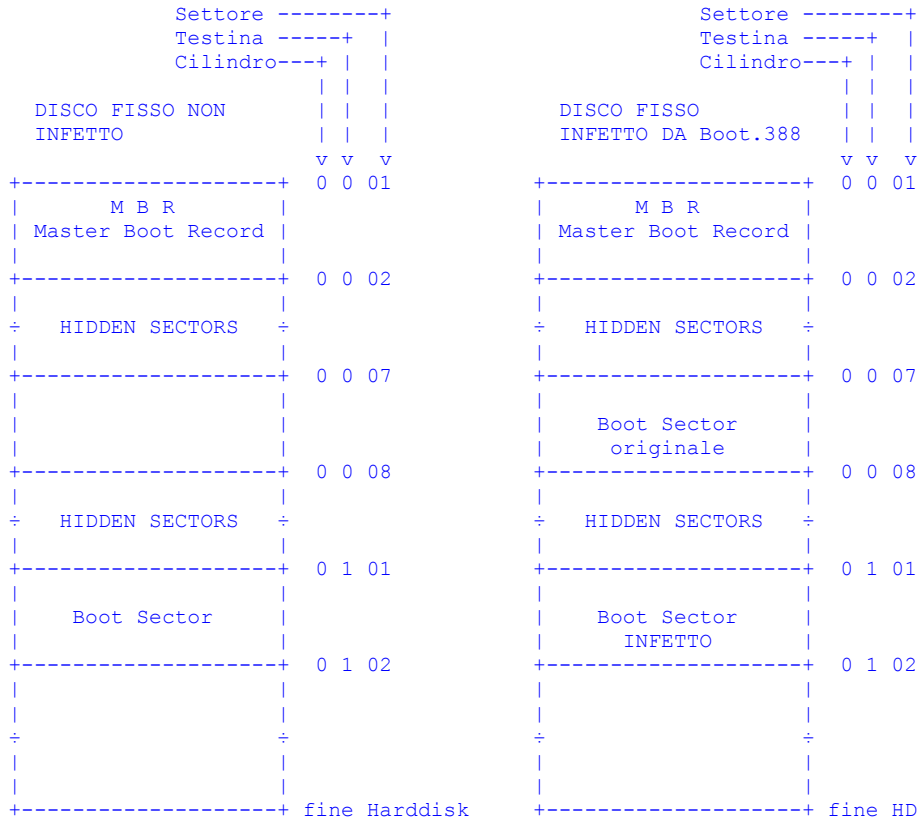
Boot.388

di Gianfranco Tonello

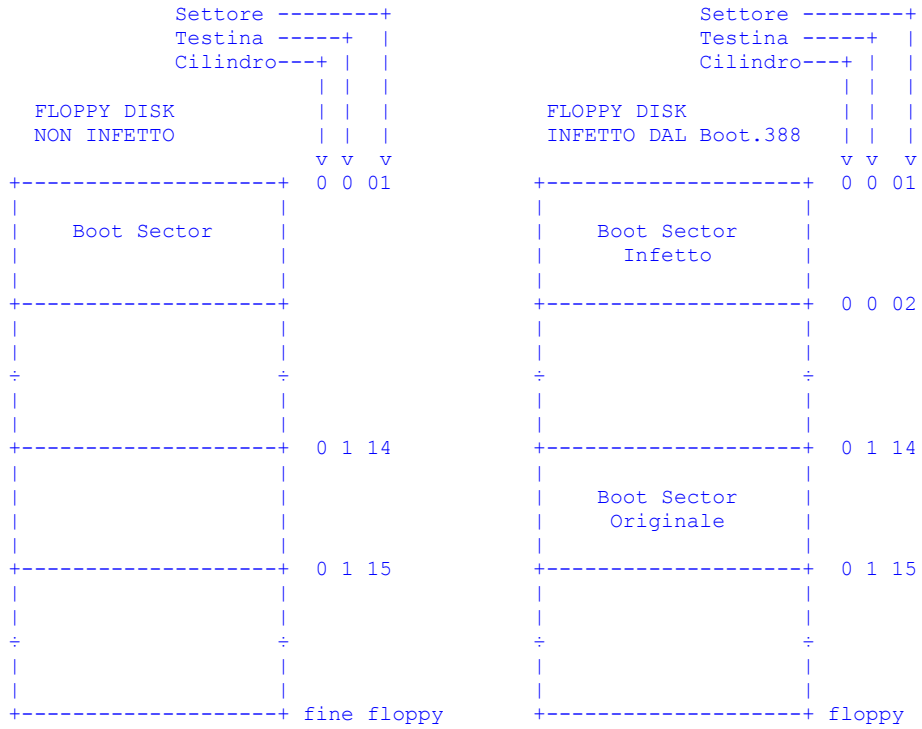
Nome virus:	Boot.388
Aliases:	
Variante:	
Stato:	
Isolato:	Maggio 1996, Aosta (Italia)
Sintomi:	diminuzione della memoria libera del sistema
Origine:	Italia (?)
Dimensione:	388 bytes
Tipo:	Residente in memoria, infetta il boot sector;
Analisi a cura di:	Gianfranco Tonello (e-mail: tge@maya.dei.unipd.it)

COMMENTO GENERALE

Il virus Boot.388 è stato isolato nel mese di Maggio 1996 in Italia (Aosta), la sua origine potrebbe anche non essere italiana. Il codice virale risulta essere residente in memoria (TSR), infetta il boot sector dei floppy disk e del disco fisso. Quando il Boot.388 si attiva dal boot dei floppy disk, si alloca in memoria, la memoria libera del sistema diminuisce di otto kilobytes. A questo punto viene intercettato l'interrupt 13H (Disk/Diskette Services) e infettato il boot sector del disco disso. Il Boot sector originale del disco fisso viene salvato nel settore 7, testina 0 e cilindro 0.



Ogni floppy disk, che verrà inserito nel drive 0, non protetto in scrittura, sarà infettato dal virus Boot.388 nel modo seguente:



Il virus Boot.388, salva il boot originale nel settore 14, cilindro 0, testina 1, alcuni formati dei floppy hanno solo 9 settori per traccia, quindi non viene salvato il settore originale. Ad esempio nei floppy disk da 1.44Mb viene salvato il boot originale, invece nei floppy da 720Kb questa operazione fallisce. Il codice virale Boot.388, si attiva il 20 marzo di ogni anno sovrascrivendo 5 settori alla volta, partendo dal settore 1, cilindro 0 e testina 1 con valori casuali.

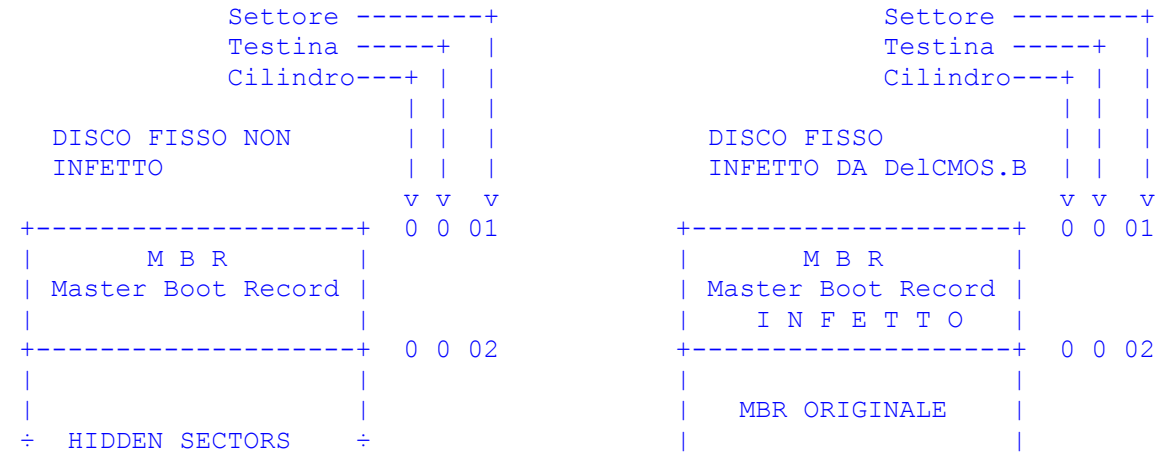
DelCMOS.B

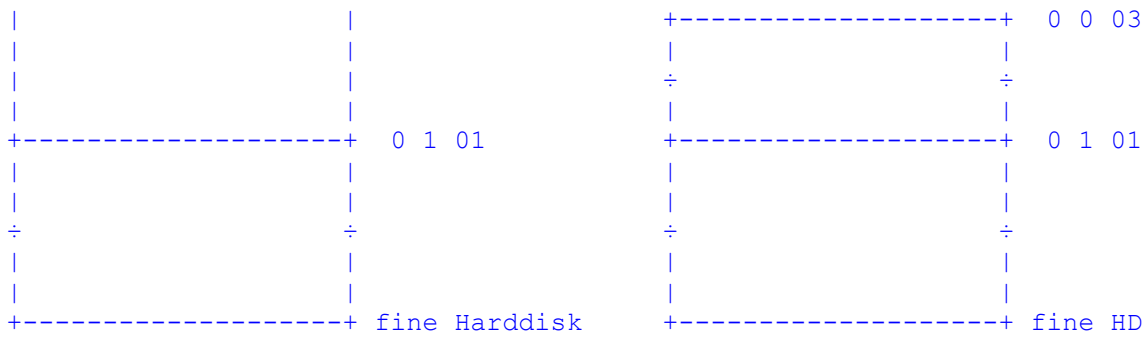
di Gianfranco Tonello

Nome virus: DelCMOS.B
Aliases:
Variante:
Isolato:
Sintomi: diminuzione della memoria libera del sistema
Origine:
Dimensione: 1 settore
Tipo: infetta boot sector e MBR
Analisi a cura di: Gianfranco Tonello (e-mail: tge@maya.dei.unipd.it)

COMMENTO GENERALE

Il codice virale DelCMOS è un virus residente in memoria, stealth, infetta il master boot record del disco fisso e il boot sector del floppy disk. Quando il DelCMOS.B si attiva dal boot dei floppy disk, si alloca in memoria all'indirizzo 9F80:0, la memoria libera del sistema diminuisce di due kilobyte. A questo punto viene intercettato l'interrupt 13H (Disk/Diskette Services) all'indirizzo CS:00A3H e infettato il Master Boot Record (MBR) dell'hard disk. L'infezione del Master Boot Record è similare a quella addottata dal molti codici virali che infettano l'MBR. Il virus DelCMOS.B quando infetta il master boot record (cilindro 0, testina 0, settore 1) del disco fisso, salva l'MBR originale nella posizione: cilindro 0, testina 0, settore 2. Il codice virale infetta l'hard disk nel seguente modo:





Ogni floppy disk, che verrà inserito non protetto in scrittura sarà infettato dal virus DelCMOS.B. Non tutti i formati dei floppy disk vengono infettati. Il settore di boot originale viene copiato in un'area non molta sicura, che può essere sovrascritta quando l'utente copia dei files all'interno del floppy disk. Una caratteristica del codice virale è quella di essere invisibile (stealth) quando è residente in memoria, cioè in questa situazione andando a leggere il master boot record del disco fisso, il virus mostrerà il settore originale, quello non infetto.

Collabora con Italian VIRUS Magazine

Sei un ricercatore Anti-Virus, sei in grado di analizzare un codice virale, hai notizie o informazioni riguardanti i virus informatici MS-DOS, che abbiano qualche interesse per la comunità informatica italiana?
Contatta la redazione di Italian VIRUS Magazine scrivi a:

TG Soft
Via Sardegna n° 5
35030 Sarmeola di Rubano (PD)

Allega una tua presentazione e/o un tuo curriculum, nonchè una traccia del materiale in tuo possesso. Se tale materiale sarà ritenuto interessante per la pubblicazione sarai ricontattato ed invitato a scrivere un articolo.

Segnala i VIRUS circolanti in Italia

Segnalare le infezioni derivanti da virus informatici significa dare un concreto contributo alla lotta antivirale, permettendo agli sviluppatori di antivirus di mettere a disposizione dell'utenza gli antidoti per combattere efficacemente i virus più diffusi in Italia.

Come si segnalano i virus circolanti

Le infezioni informatiche in atto sono da segnalare con le seguenti modalità:
- a mezzo telefono allo 049-631748 (TG Soft - ore ufficio)
- a mezzo Fax allo 049-631748
- telematicamente in INTERNET all'indirizzo e-mail: tge@maya.dei.unipd.it

Saranno gradite le seguenti informazioni:

```
Nome Virus: ____________________ Anti-virus rilevatore: ________________
N.Computer colpiti: _____ Data __-__-__ Provincia: ____________________
Azienda: [  ]                           Privato: [  ]
```

VirIT Lite

L'antivirus gratuito sia per i privati che per le aziende

Molti utenti sono convinti che programma shareware significhi gratuito, può sembrare superfluo ricordare che non è così. Inoltre molti programmi distribuiti come shareware, hanno questa caratteristica quando sono usati da utenza PRIVATA, mentre in ambito AZIENDALE il loro uso senza la relativa LICENZA non è autorizzato. Questa situazione è tipica per molti prodotti antivirus tra i più noti. Molti, anche in ambiti aziendali, li utilizzano indiscriminatamente per lunghi periodo credendo (a torto) di essere in FASE di VALUTAZIONE. Generalmente le istruzioni che compaiono all'attivazione del software vengono ignorate (vuoi perchè in lingua inglese, vuoi per la fretta di utilizzare il programma), queste spiegano chiaramente che l'utilizzo AZIENDALE è consentito solamente se il software è munito di regolare LICENZA d'USO.

VirIT -Il Servizio Antivirus italiano- ha pensato di risolvere questo "problema" realizzando una versione GRATUITA, sia per i PRIVATI che per le AZIENDE del software antivirus VirIT, chiamata VirIT Lite.
VirIT Lite è liberamente utilizzabile e distribuibile senza scopo di lucro, viene distribuito come file VLT-*.ZIP (es. VLT-104.ZIP etc. etc.), ed è facilmente reperibile.***

Dove trovare VirIT Lite

- in INTERNET presso il sito FTP.FUNET.FI nella directory \pub\unix\security\docs\TGSoft
- in tutti i nodi della rete VIRNET e I.S.N. (Italian Shareware Network)
- presso C.R.A.V. BBS Tel. 049-8977596 (da lunedi a venerdi dalle 8,30 alle 19,00)
- richiedendolo a TG Soft Tel. 049-631748 (ore ufficio)

Index

≡
#
A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V
W
X
Y
Z

Introduzione

IVP

N

NEWS

NGRL

P

PSMPC

R

Redazione

S

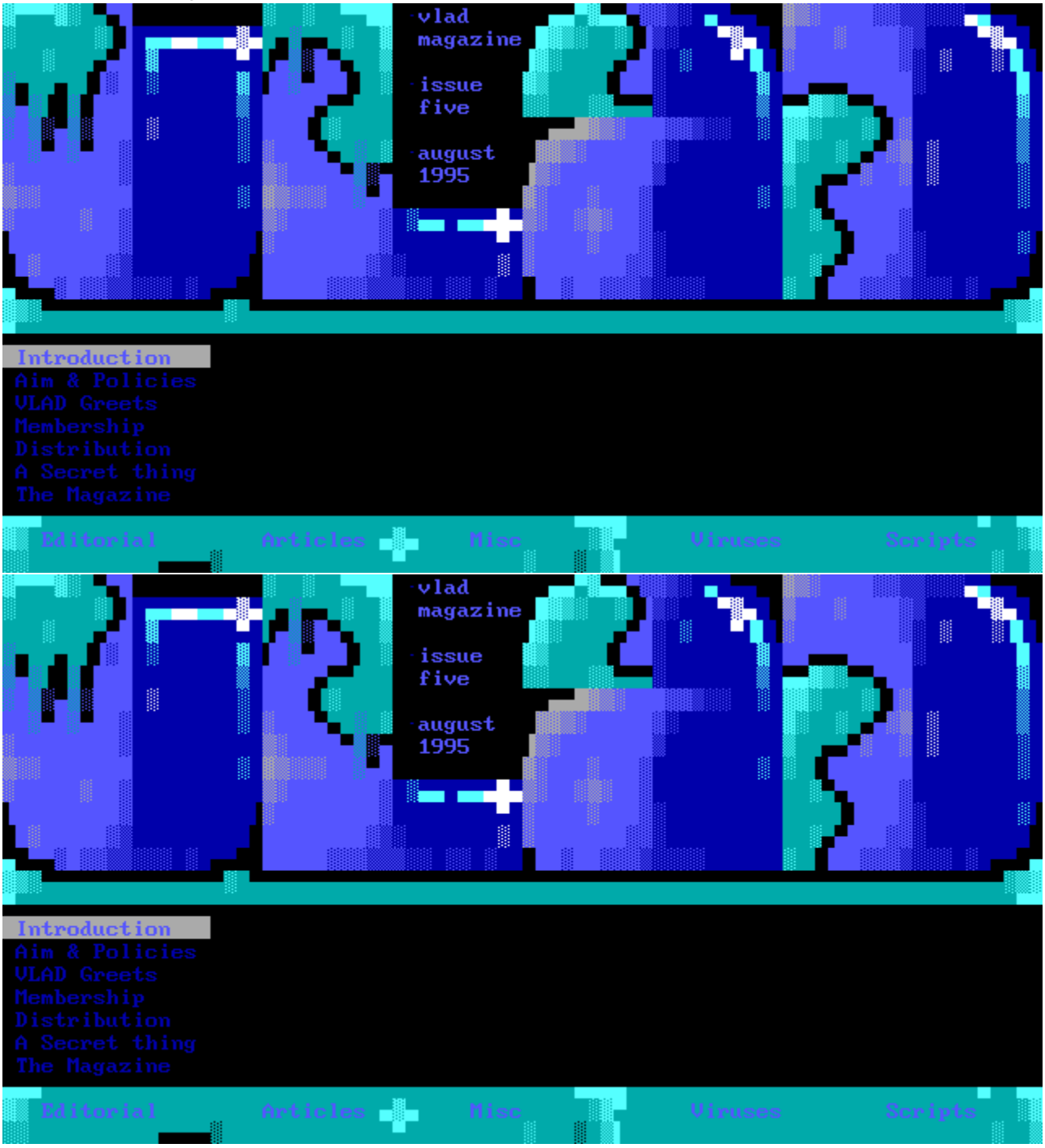
SEGNALA_INFEZIONI

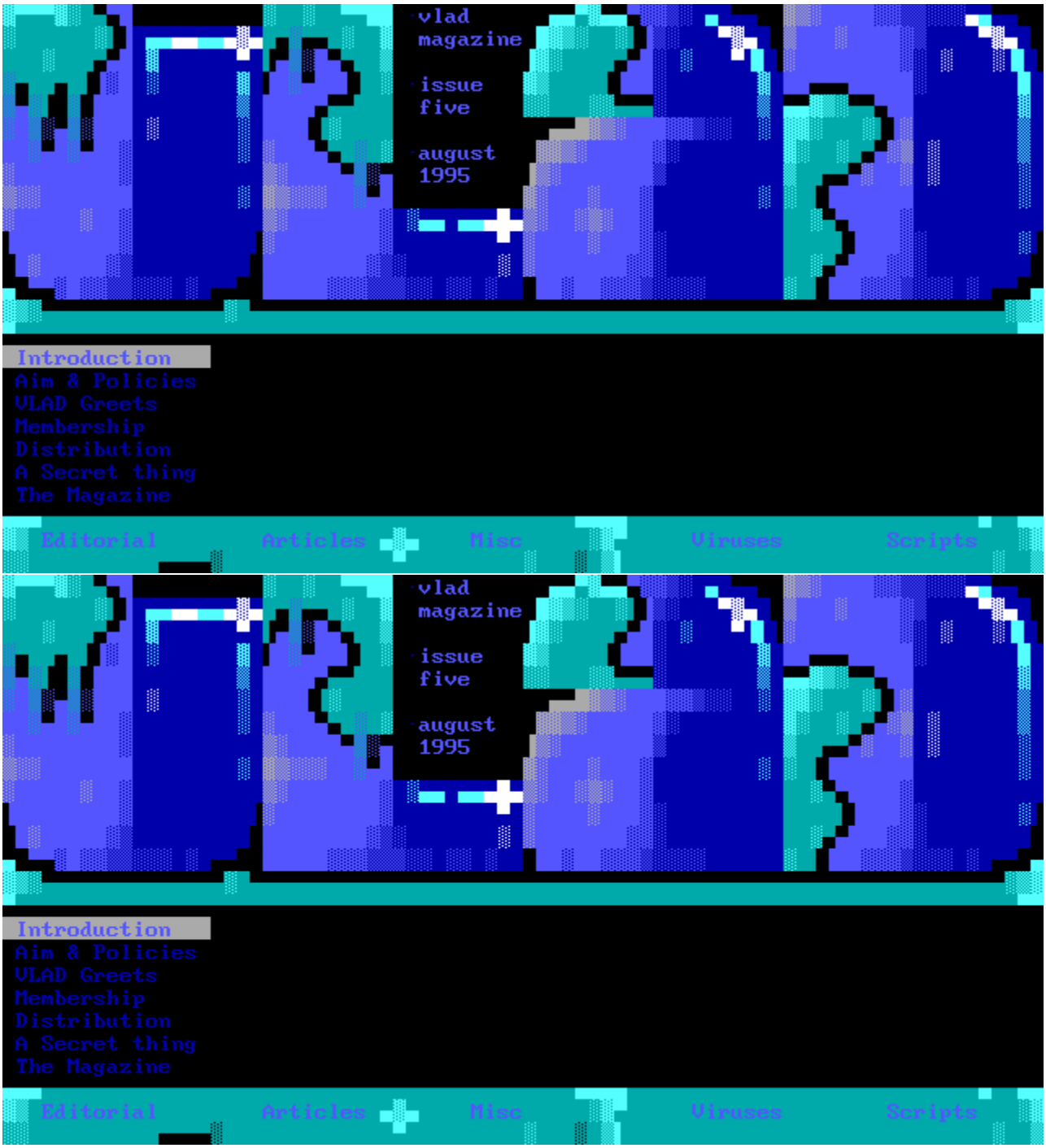
V

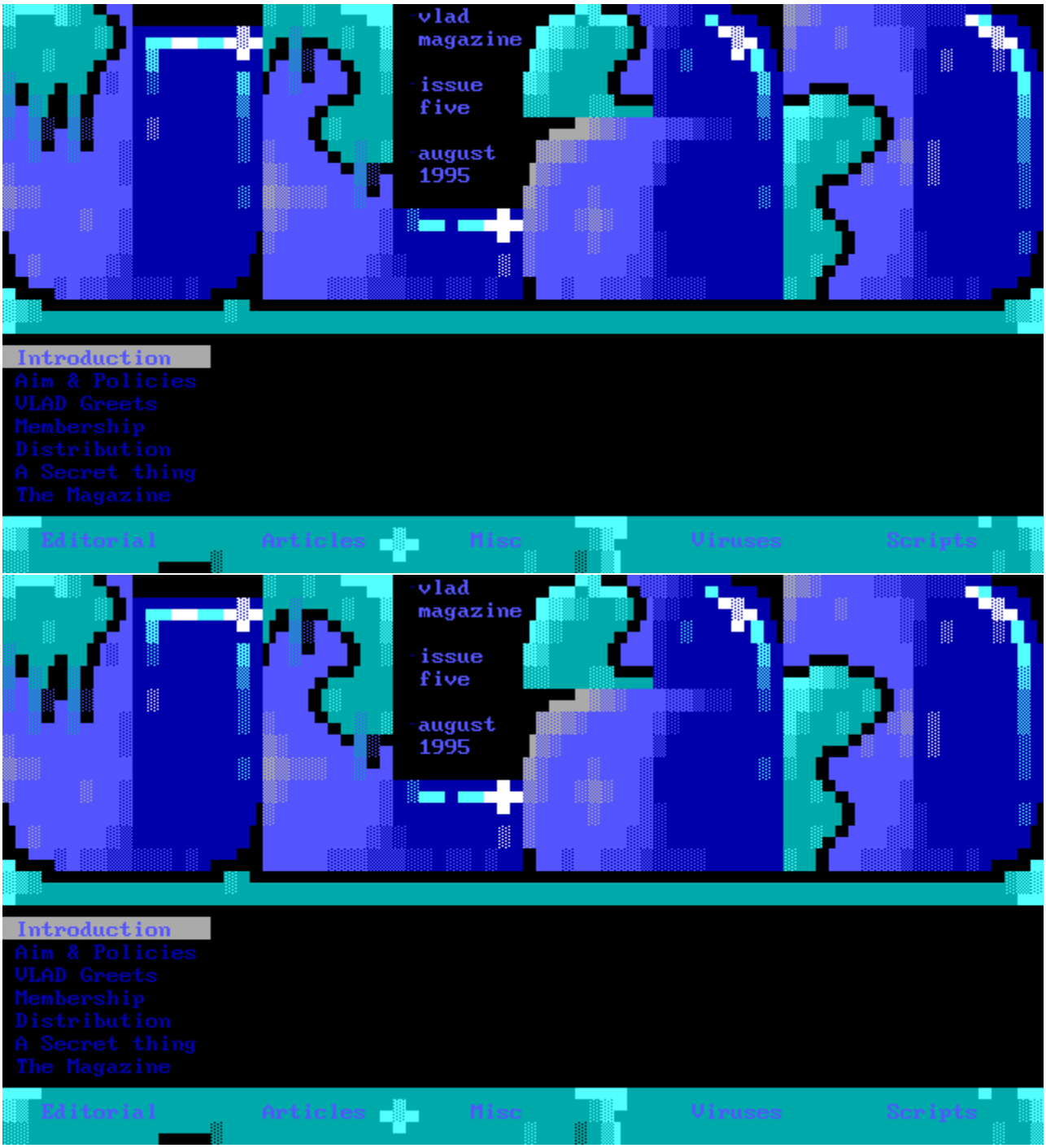
VirIT Lite

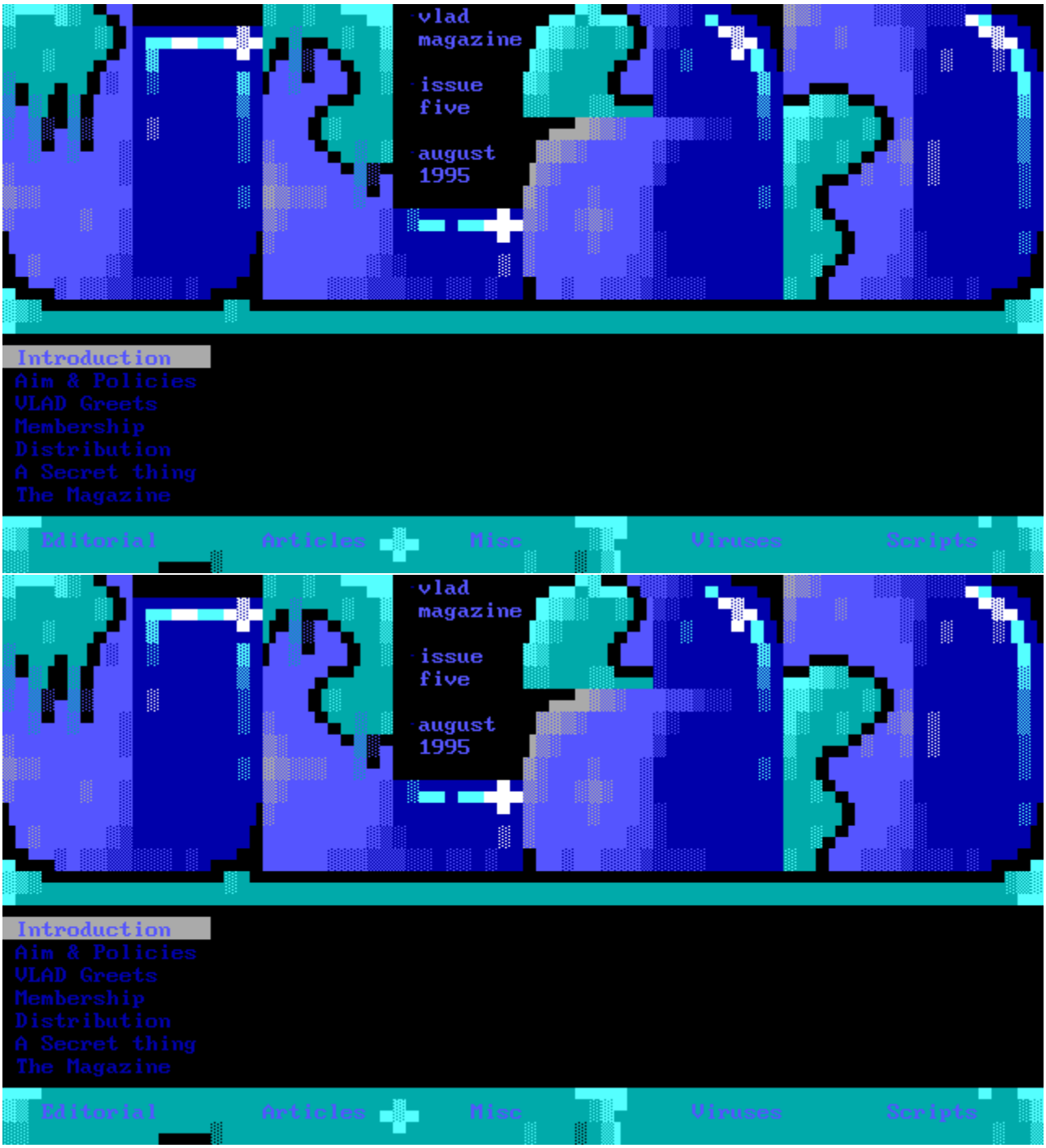
vlad

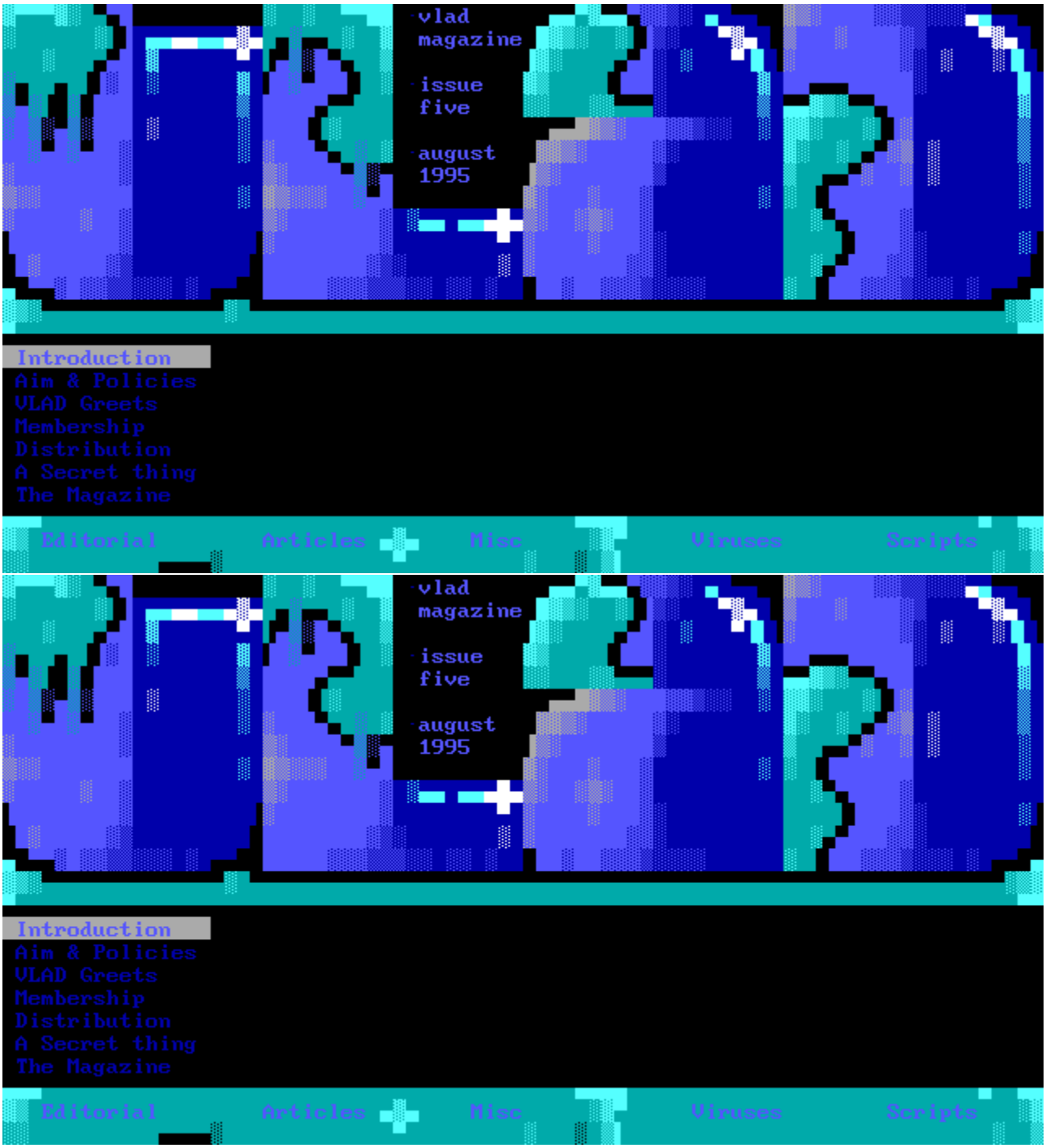
Glossary

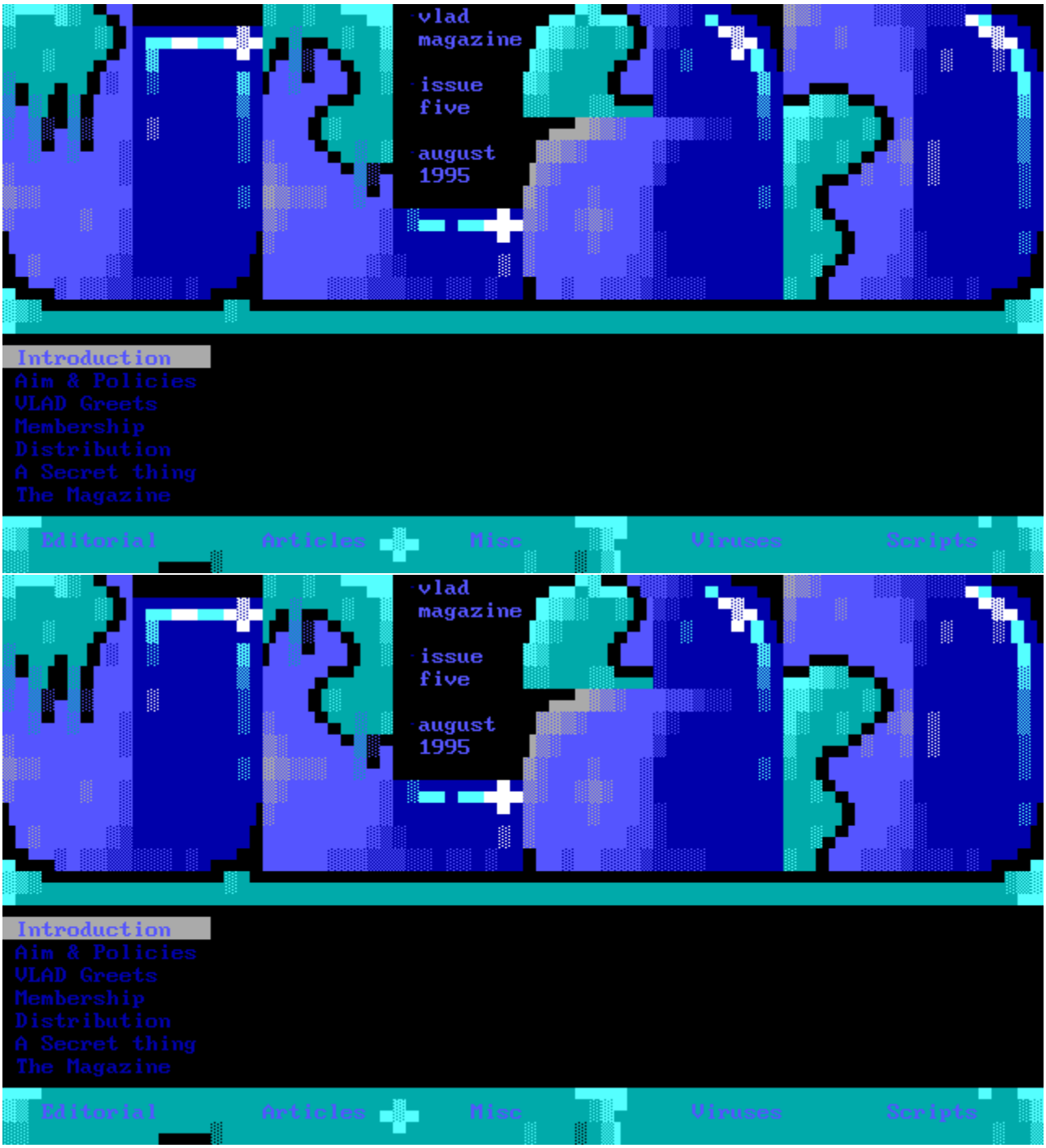

vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts
vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts

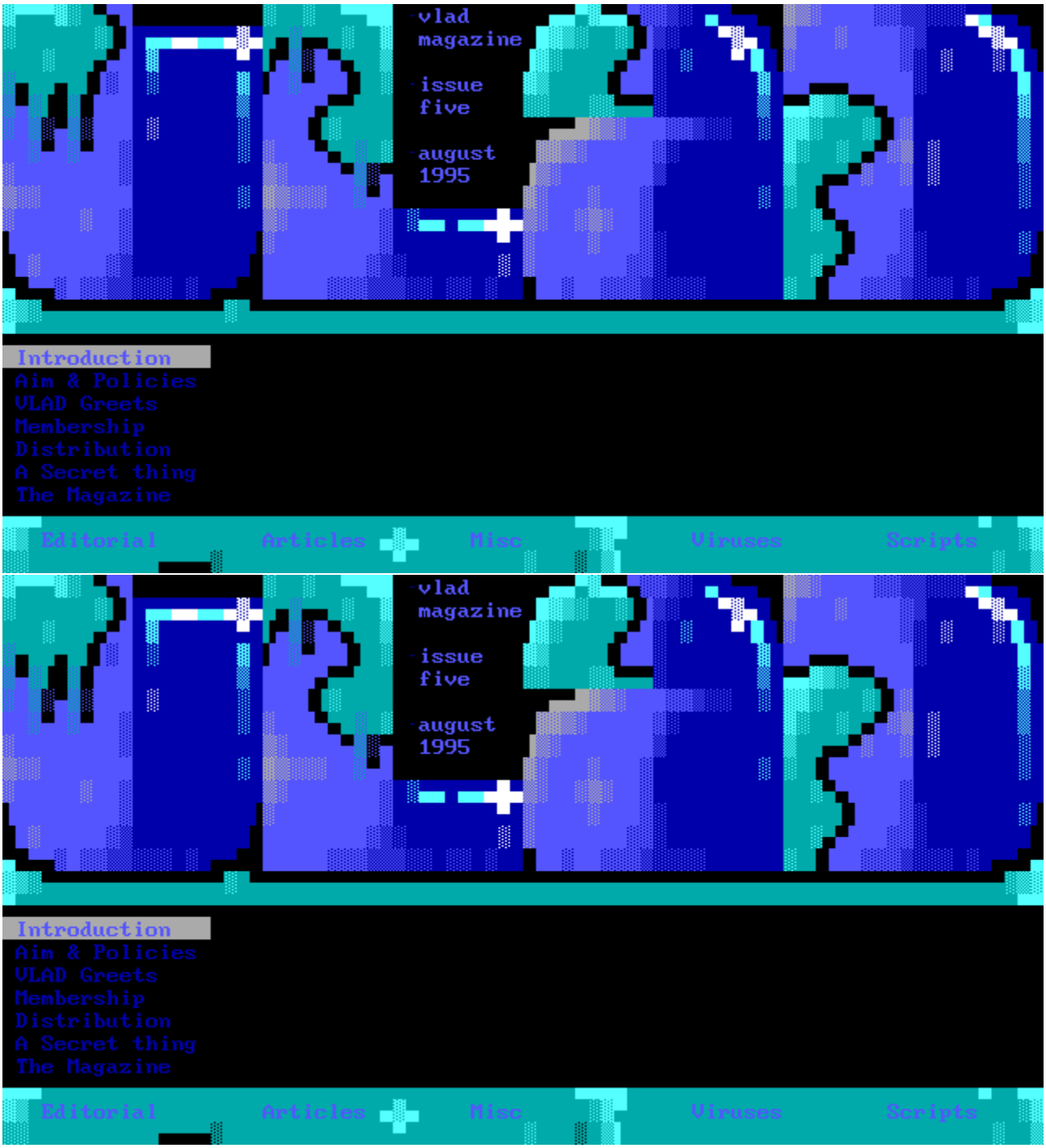

vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts
vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts

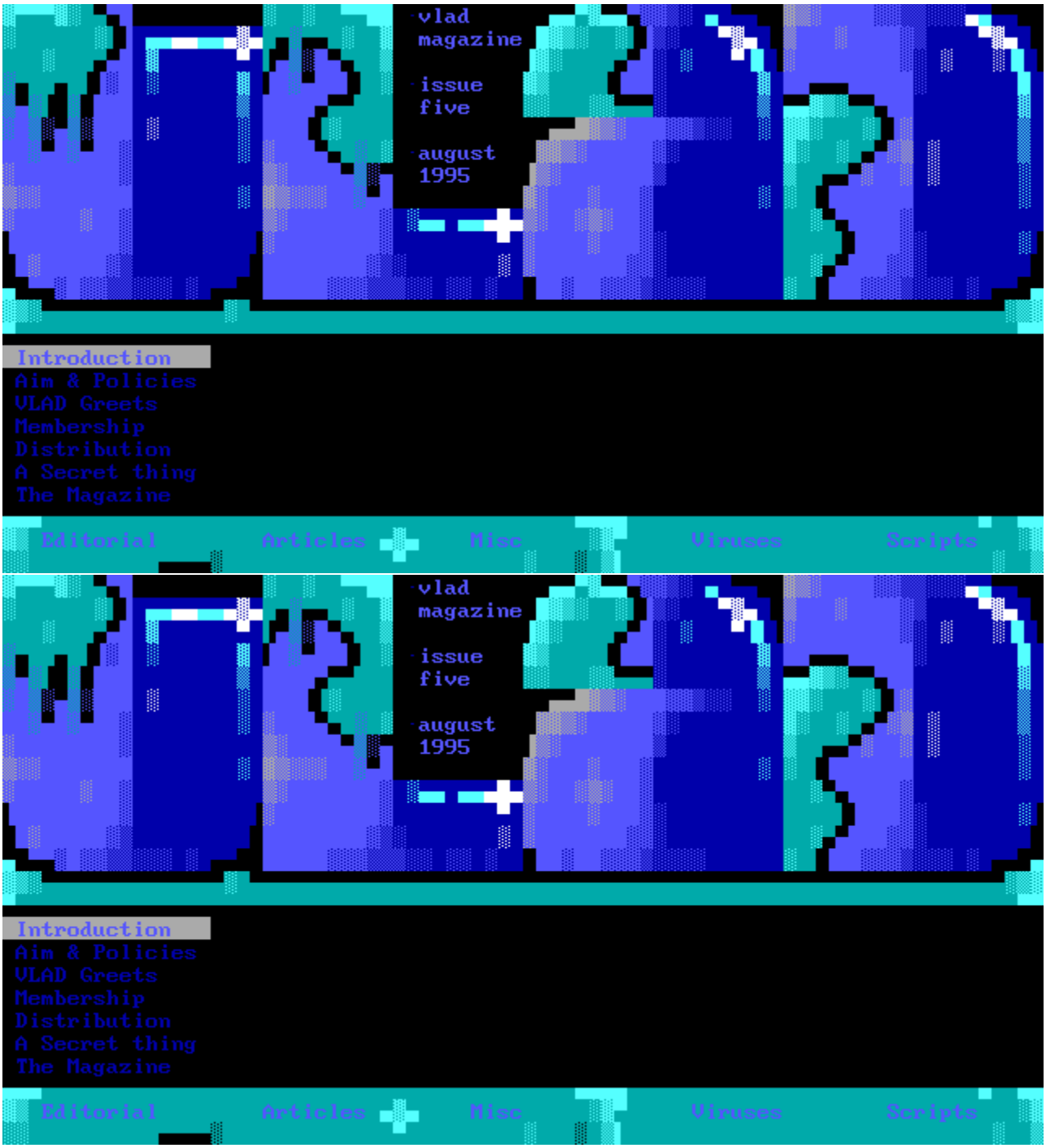

vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts
vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts

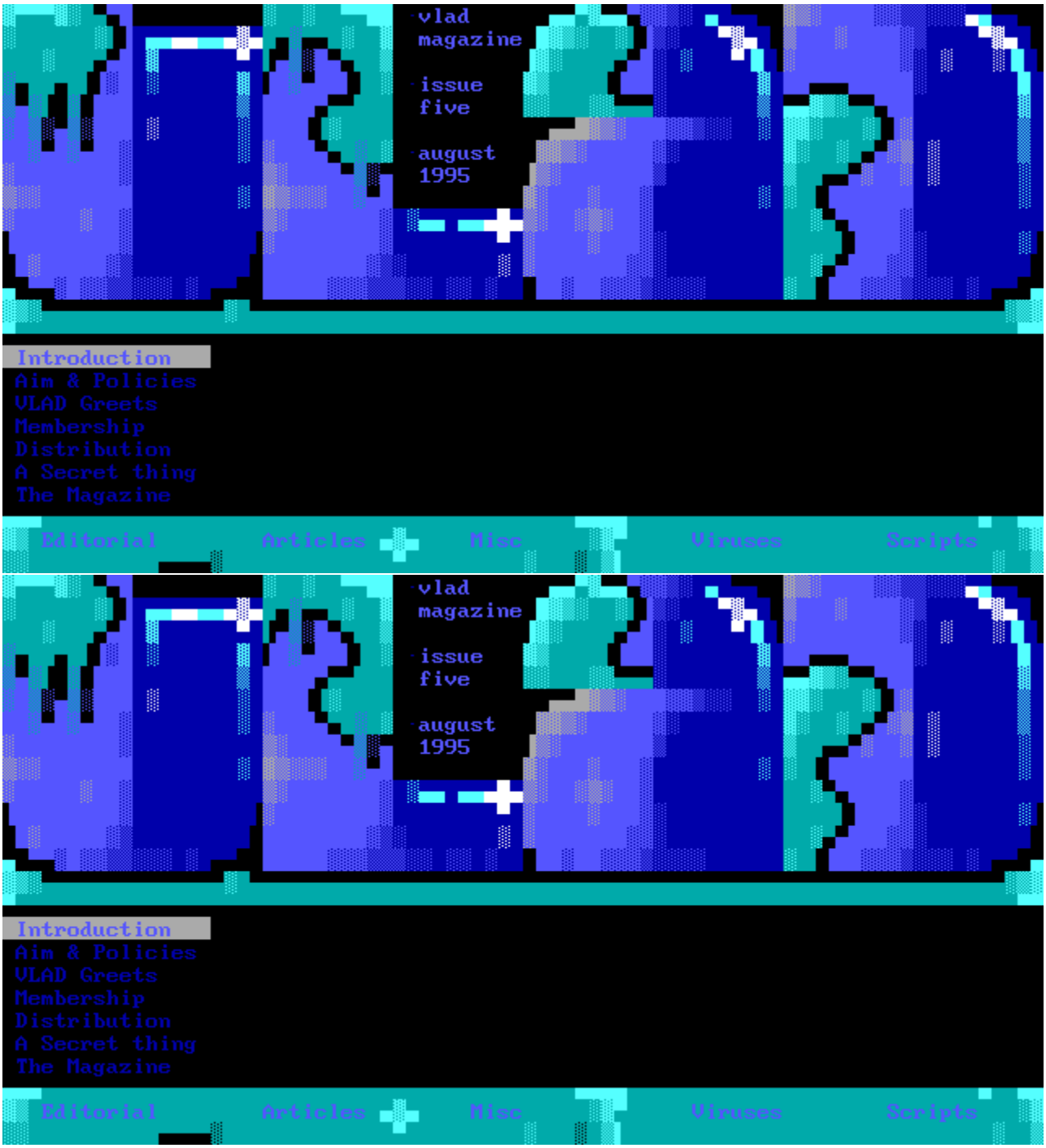

vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts
vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts

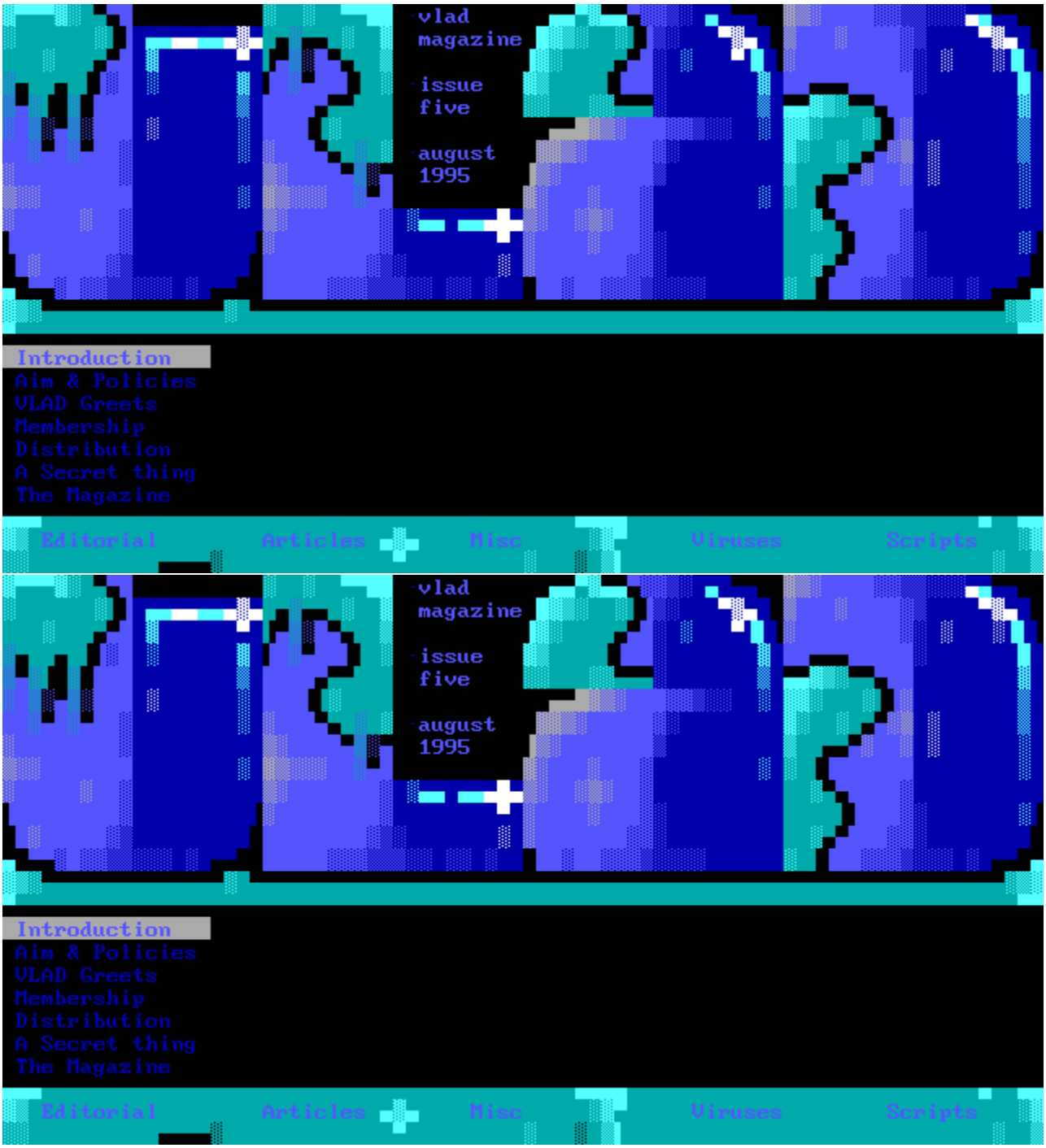

vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts
vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts

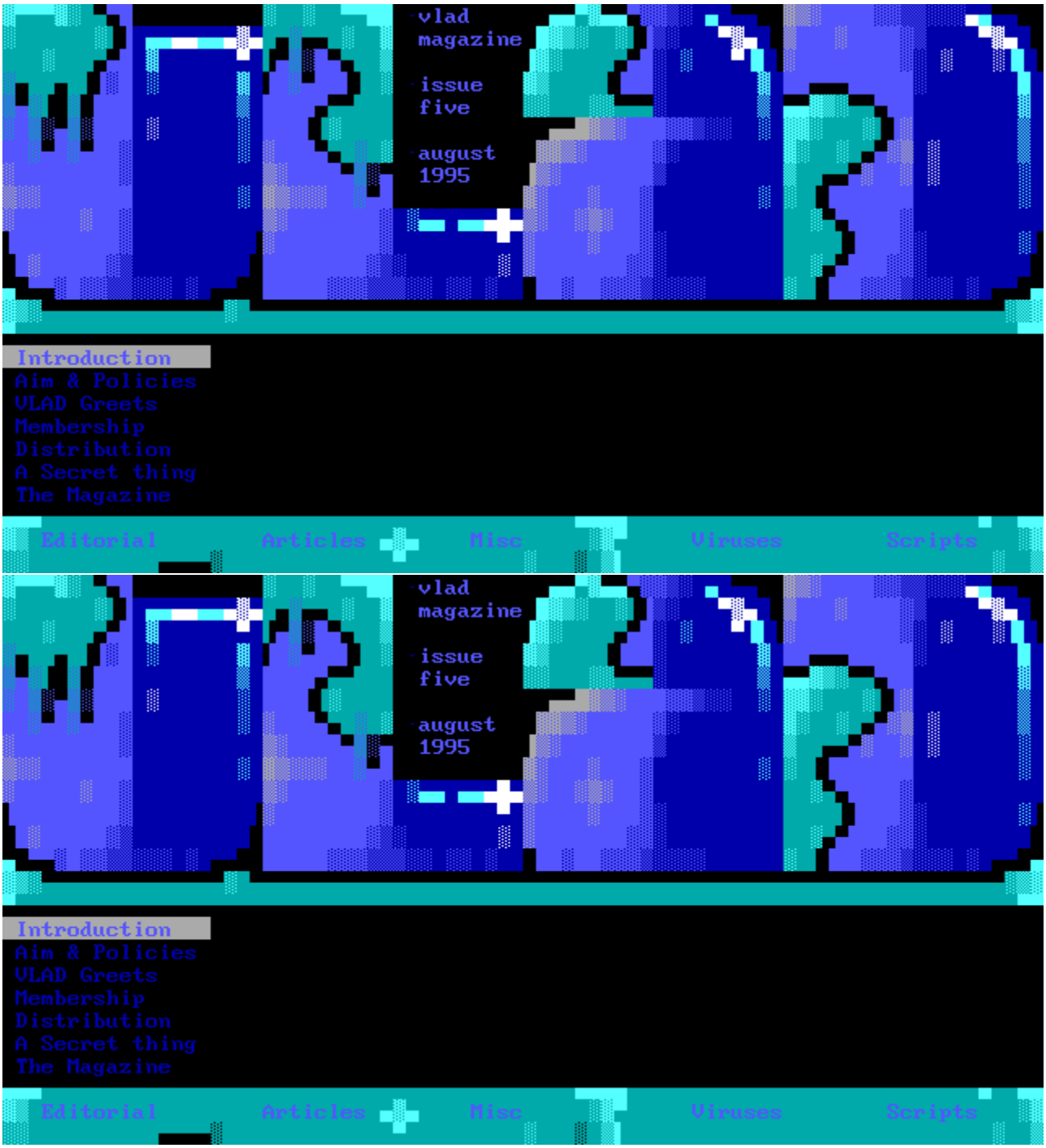

vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts
vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts

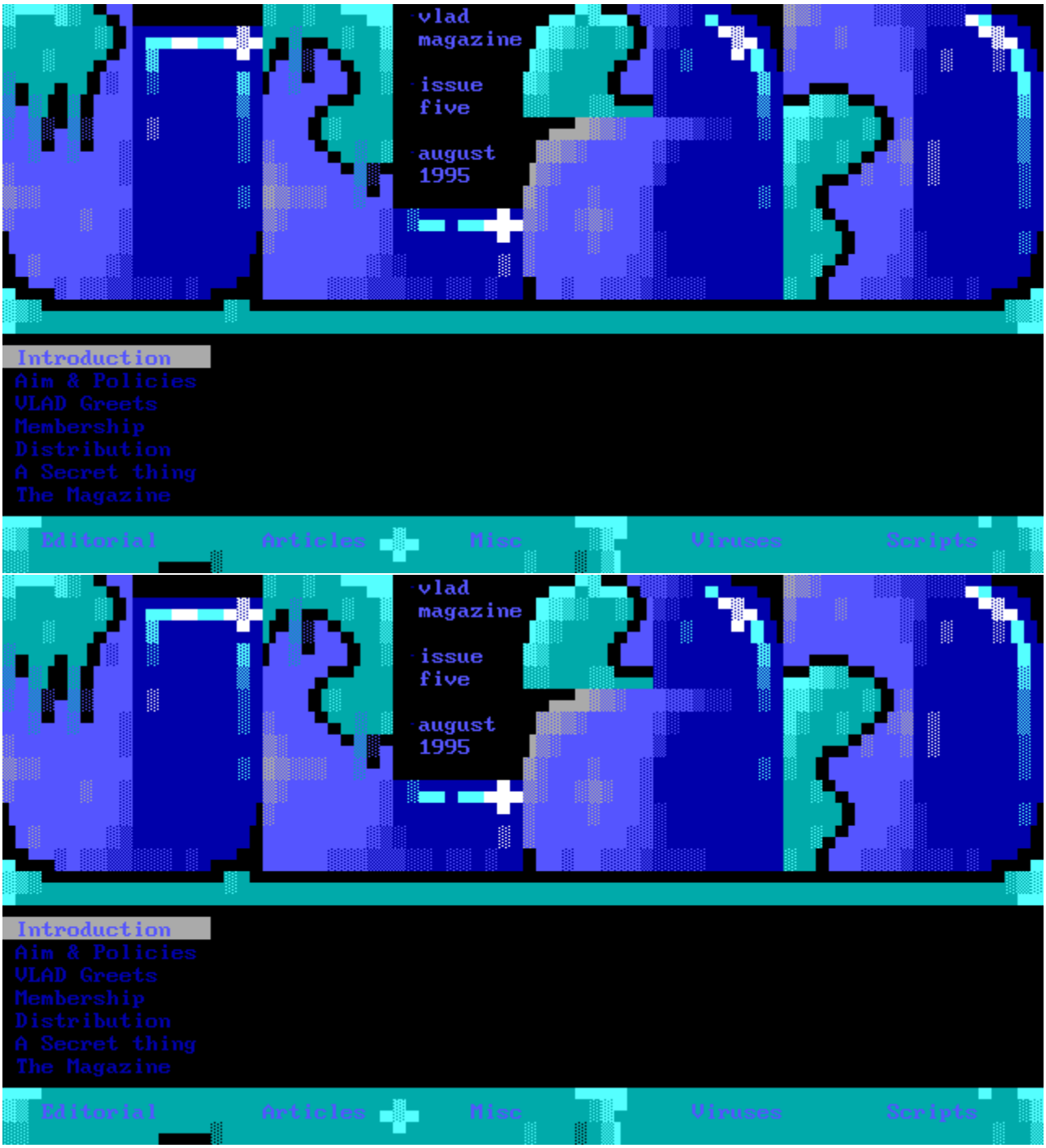

vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts
vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts

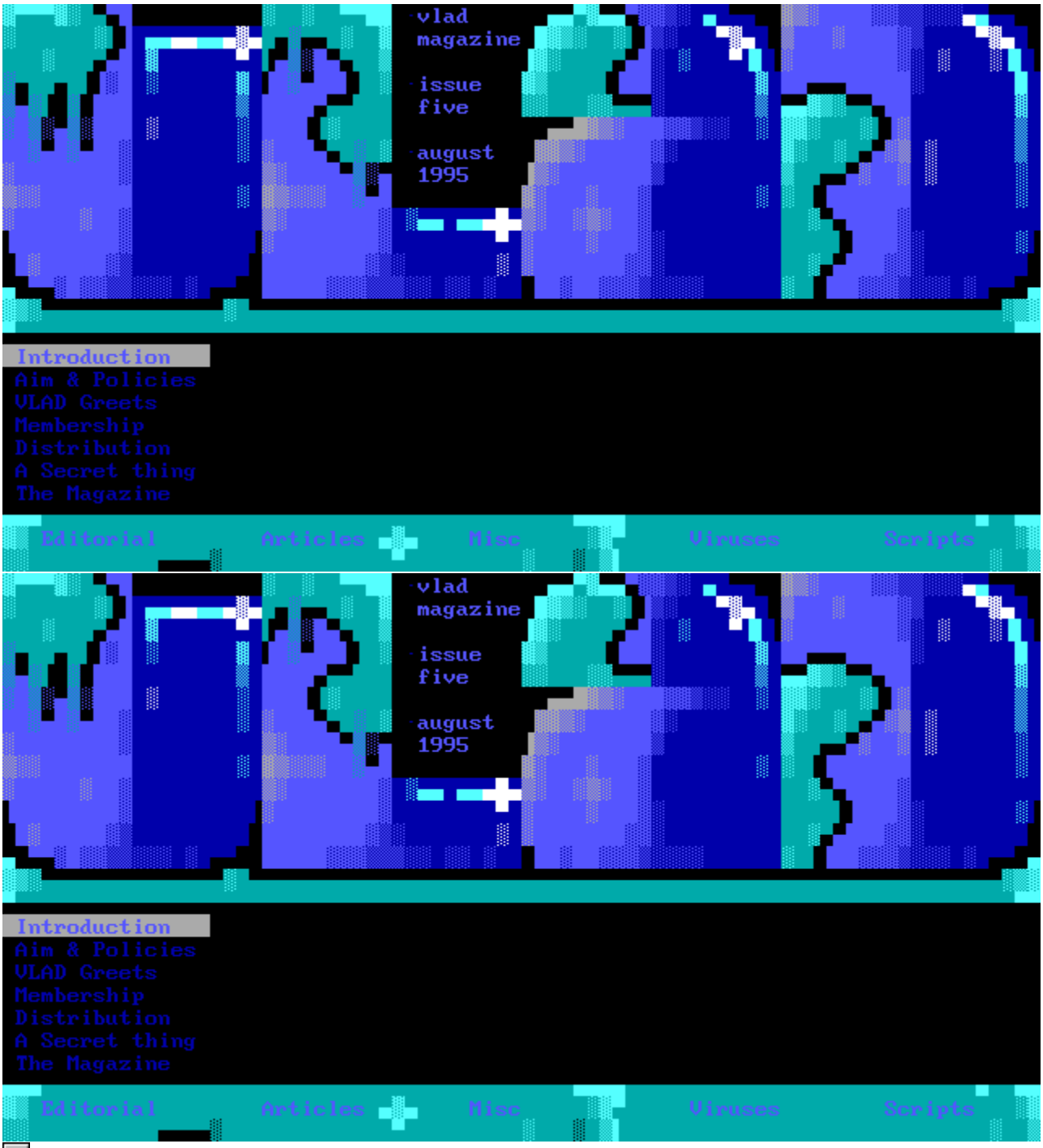

vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts
vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts


vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts
vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts


vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts
vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts


vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts
vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts


vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts
vlad
magazine
issue
five
august
1995
Introduction
Aim & Policies
VLAD Greets
Membership
Distribution
A Secret thing
The Magazine
Editorial
Articles
Misc
Viruses
Scripts



Y

Z

C

Cavallo di troia

CODICI VIRALI

E

Enrico Tonello

EURISTICO

F

Federico Pellegrin

FIRME VIRALI

G

Gianfranco Tonello

S

Shareware

Stealth

T

TG Soft

TROJAN

V

virus

Cavallo di troia

Trojan horse, o cavallo di troia:Programma che nasconde sotto una facciata innocua ed invitante un programma killer che generalmente distrugge i dati dell'hard disk

CODICI VIRALI

Sinonimo di virus informatico, ossia il vero e proprio programma che é in grado di autoreplicarsi.

Enrico Tonello
Curatore delle Pubbliche Relazioni della TG Soft. Consulente di sicurezza informatica in materia antivirale in ambito bancario ed aziendale. Può essere contattato allo 049-631748 (ore ufficio).

EURISTICO

Metodo che consente di determinare se un programma esegue operazioni sospette, ossia operazioni tipiche dei virus informatici permette pertanto di intercettare dei virus di cui non si conosce ancora la firma virale.

Federico Pellegrin
Appassionato sulle problematiche generate dai virus informatici.

FIRME VIRALI

Il codice esadecidemale che permette di identificare il virus. I virus polimorfici cercano di automodificarsi per non farsi intercettare dai comuni antivirus.

Gianfranco Tonello
Esperto di sicurezza informatica in ambito bancario ed aziendale, sviluppatore del software anti-virus VirIT & VirIT Lite e coordinatore di VirIT -Il Servizio Antivirus aziendale-. E' contattabile in INTERNET all'indirzzo e-mail: tge@maya.dei.unipd.it

Shareware

modalità di distribuzione, che prevede la possibilità di provare il software prima di acquistarlo (try before you buy). L'utilizzatore dopo aver provato il software (per il periodo prescritto), se lo ritiene utile per la sua attività, e quindi decide di continure ad utilizzarlo dovrebbe registarsi inviando all'autore la somma richiesta.

Stealth

viene definito in questo modo un codice virale che ha la capacità di mostrare la situazione antecedente all'infezione, quindi di non farsi individuare (invisiblità).

TG Soft

Software house specializzata in Sicurezza Informatica con particolare attenzione nel campo della lotta anti-virale in ambiente MS-DOS, realizzatrice di VirIT -Il Servizio Antivirus italiano- l'unico servizio antivirus realizzato interamente in Italia, costituito da un pacchetto software e da servizi di complemento di provata efficacia in ambito bancario ed aziendale. Per ulteriori informazione Tel./Fax 049/631748 (Fax 24h/24).

TROJAN

Trojan horse, o cavallo di troia:Programma che nasconde sotto una facciata innocua ed invitante un programma killer che generalmente distrugge i dati dell'hard disk

virus
Programma in grado di autoreplicarsi.