

A MatrixMage Electronic Publication

Special Thanks to the Following Contributors:

Z Maestro RA of ISCA Underground>
DINO RA of Shadow Hack and Crack>
Artimage RA of SKYNET Underground>

Faunus	Revolution	Miska	Informatik
Matrixx	Amarand	Crypto Steelyhart	aBBa / PFA
Beelzebub	Redbeard	Squarewave	
IO	CyberSorceror	Caustic	
Doktor Nil	Skipster	Walrus	
CPT Ozone	Abort	Kyoti	
Carsenio	Aero	Phrack	

AND NOW A WORD FROM YOUR EDITOR:

Throughout history mankind has been afraid of the unknown. Before lightning could be scientifically explained it was blamed on the anger of the gods. This belief in mysticism persisted throughout the ages (and still does today). Later as man acquired simple herbal and chemical knowledge, these men were revered as mages, users of mystical arts derived from the old gods. But as organized religion (i.e. Christianity especially Roman Catholicism) spread and came to dominate society (became the powers that be), the mage was no longer revered. The mage (who only sought to understand the world around himself and make the world a better place) was persecuted, attacked and driven underground by the church. But driving these mages underground (out of society) did not stop there ideas from spreading or them from continuing to work. The church label Copernicus as a heretic and mage and only this century has the Roman Catholic church accepted his principles (heliocentric universe) as fact.

So are 'hackers' the same today. We surf the nets seeking knowledge and information (and hopefully understanding). Information and understanding the meaning and import of the information are the two greatest commodities and bases of power in the world today. These things are easy to disseminate and gather in the electronic world. The matrix (cyberspace/web/net [whichever term you choose] is able to influence and control information faster and better than ever before. This makes many afraid of the cyberculture (not to mention a deep-seated techno-fear of many people, anything new and technical is bad).

We are a new breed of mage; seeking knowledge, desiring understanding, persecuted by the powers that be. This is why I have started this publication. We are the MatrixMages! Our mission is to learn and to pass on that knowledge.

--> Belisarius <--

What is 'Cyberpunk' and the Underground?

"Every time I release a phile, or write an article for a zine, it's vaguely like a baby. It gets stored, and copied, and sent out all over the world, and people read it. It goes into their minds. Something I created is buried in living tissue and consciousness someplace. Eventually somebody uses it, and I know that I have the power to change the world. Somewhere, someplace, somebody changed something using information I changed or created. I helped to change the world." --Unknown

That is the attitude of many of the people who, knowingly or not, are members of this hyped/wired/cyber culture. Some who may read this will see some of their undefined beliefs, hopes and feelings reflected in the above quote. And, as the quote says, they will help spread it. Somewhere, somehow, that quote will change the world.

But only if you work to change it. Remember that information and knowledge a powerful commodities. He who has information cannot be beaten. So above all the most important thing to do in the "Underground" is to gather information. This means that you have to work and put in some effort. You don't get something' for nothing! So work hard and together we can change the world!

Keep up with latest editions. (Sorry there haven't been many lately but exams and not failing out took precedence!)

The Haq, MatrixMage, THE HACK-FAQ!, Belisarius, Neurophyre, or any contributor are not responsible for any consequences. You use this information at your own risk.

CONTENTS

Sections

- I. Phone Fun
(Red Boxing, COCOTS, Beige Boxing, Cellulars, etc.)
- II. Fake E-Mail
(Fooling UUCP)
- III. Social Engineering
(Free sodas, Dumpster Diving, ATMs, Carding)
- IV. The Big Bang
(Making Weapons and Explosives)
- V. Infection
(Virii, Trojans, Worms and other creepy crawlies)
- VI. NEWBIES READ THIS
(Basic Hacking)
- VII. Screwing with the most widespread operating system on the net
(UNIX / AIX Hacking)
- VIII. Screwing with the most secure operating system on the net
(VAX/VMS Hacking)
- IX. Screwing with the most widespread operating system on PCs
(MS-DOS Hacks)
- X. Finding out what that encrypted info is
(Cracking programs)

- XI. How do I keep my info secure
(PGP / Cryptology)
- XII. Chemistry 101
(explosive/pyrotechnic component prep)
- XIII. Fun things with solder, wires, and parts
(Underground electronics)
- XIV. Watching television
(cable, Pay-Per-View(PPV), scrambling)
- XV. Tuning in to what's on the radio waves
(Radios and Scanning)

Appendices

- A. FTP sites with useful info
- B. Interesting Gophers
- C. Informative USENET Newsgroups
- D. Publications and Zines
- E. Books
- F. Files and Papers
- G. Cataglogs
- H. PGP Keys

=====

I. Phone Fun

(Red Boxing, COCOTS, Beige Boxing, Cellulars, etc.)

WHAT IS A RED BOX AND HOW DO I MAKE ONE?

(from Doktor Nil)

First note: a redbox is merely a device which plays the tone a payphone makes when you insert money. You just play it through the mike on the handset. You would think that the Phone Co. would mute the handset until you put a quarter in, and perhaps they are starting to build phones like that, but I have yet to see one.

What you need:

- Radio Shack 33 memory Pocket Tone Dialer
- 6.4 - 6.5536 megahertz crystal (get 6.5 MHz from Digikey, address below)
- A solder gun.
- Someone who can point out the crystal in the Tone Dialer.

Instructions:

1) Open up the back of the tone dialer. Use screwdriver.

2) Locate crystal. It should be toward the right side.

It will be smaller than the 6.5 MHz one you bought, but otherwise vaguely similar. It is basically capsule-shaped, with two electrodes coming out of the bottom which are soldered onto a circuit board. It's on the left side, basically the third large crystal thing from the bottom, about 1.5 cm long, metallic, thin.

3) De-solder, and de-attach, crystal. Heat the solder that the

sized gray or black boxes that appear where a single phone line meets the mother line. They look almost like outdoor electric sockets, that have the snap up covering. They normally have the letters TTI somewhere on the front. No bolts or screws to take off, just snap up the top and you will see four screws. Clip in and happy phreaking. Just click the top down and no one will ever know you were there (except for the extra digits on their phone bill.)

Green trees: just about the hardest sw. ap. to beige from (tied with the bell canister) but if its the only one you can use, go for it. These are the 3 foot high green/gray metal columns that are no wider than a telephone pole (which makes them different then the green bases, see below), that say "Call before digging, underground cable," or the real old ones just have a bell sign. Usually green trees are right at the base of phone poles, or within a foot or two of them. These normally have two 7/16 bolts on one side of the column, which have to be turned 1/8 a turn counterclockwise, and the front of the base will slide off. Now you will see a sheet of metal with a few square holes in it, that has a bolt where the doorknob on a door would be. Ratchet this one off and the metal sheet will swing open like a door. On one side of the sheet will be a paper with a list of #'s this tree connects to. Inside you'll see a mass of wires flowing from gray stalks of plastic in sets of two. The whole mass will have a black garbage bag around it, or some type of covering, but that shouldn't get in the way. The wires come off the gray stalk, and then attach to the screws that you can beige from, somewhere near the ground at the center of the tree. These are on a little metal column, and sometimes are in a zig-zag pattern, so its hard to find the terminals that match in the right order to give you a dial tone.

Green bases: The gray/green boxes you see that look just like green trees, except they are about twice or three times as wide. They open the same as trees, except there are always 4 bolts, and when the half slides off, inside is a big metal canister held together with like 20 bolts. I wouldn't open it, but with a little info from friends and some social engineering, I learned that inside is where two underground phone lines are spliced together. Also inside is either pressurized gas or gel. Pretty messy.

Bell canisters: attached to phone poles at waist level. They are green (or really rusted brown) canisters about a two feet tall that have a bell insignia on the side. They will have one or two bolts at the very bottom of the canister, right above the base plate. Take the bolts off and twist the canister, and it'll slide right off. Inside is just like a green tree, except there normally isn't the list of #'s it connects to.

Mother load: Largest sw. ap. A large gray green box, like 6 x 4, attached to a telephone pole about three feet off the ground. a big (foot or two diameter) cable should be coming out the top. Somewhere on it is a label "MIRROR IMAGE CABLE". It opens like a cabinet with double doors. Fasteners are located in the center of the box and on the upper edge in the center. Both of these are held on with a 7/16 bolt. Take the bolts off, and swing the doors

number. This is the track that is used when the ATM greets you by name. There is a lot of variation in how things are ordered so occasionally you get 'Greetings Q. John Smith' or 'Greetings John Smith Q.' rather than 'Greetings John Q. Smith'. This track is also used with the new airline auto check in (PSA, American, etc).

Track 2:

The main operational track for online use. The first thing on the track is the Primary Account Number (PAN). This is usually pretty standard for all cards. Some additional info might be on the card such as expiration date.

One interesting item is the PIN (Personal Identification Number) offset. When an ATM verifies a PIN locally, it usually uses an encryption scheme involving the PAN and a secret KEY. This gives you a "NATURAL PIN" (i.e. when they mail you your pin, this is how it got generated). If you want to select your own PIN, they would put the PIN OFFSET in the clear on the card. Just do modulo 10 arithmetic on the Natural PIN plus the offset, and you have the selected PIN. The PIN is never in the clear on your card. Knowing the PIN OFFSET will not give you the PIN. This will require the SECRET KEY.

Track 3:

The "OFF-LINE" ATM track. It contains information such as your daily limit, limit left, last access, account number, and expiration date. The ATM itself could have the ability to write to this track to update information.

IV. The Big Bang

(Making Weapons and Explosives)

FLASH POWDERS:

(from Neurophyre)

Materials: Powdered magnesium, powdered potassium nitrate

1. Mix 1 part powdered magnesium and 4 parts of powdered potassium nitrate.
2. Light it with a long fuse cuz its so bright it might screw up your eyes.

REAL Cherry Bomb Powder

- 4 parts by weight of potassium perchlorate
- 1 part by weight of antimony trisulfide
- 1 part by weight aluminum powder

Relatively Safe

- 3 parts by weight of potassium permanganate
- 2 parts by weight of aluminum powder

***VERY* Shock/Friction/Static/Heat Sensitive!**

Use only if suicidal or desperate!

- 4 parts by weight of potassium chlorate
- 1 part by weight of sulfur

1 part by weight of aluminum powder

1) To use these mixtures, SEPARATELY pulverize each ingredient into a fine powder, the finer it is, the more power you get. Use a mortar and pestle if available, and grind GENTLY. Do not use plastic as this can build a static charge. Remember, do them SEPARATELY.

AMATEUR EXPLOSIVE (Ammonium Triiodide):

(from IO)

WARNING: This explosive is EXTREMELY shock sensitive when dry, and moderately sensitive when wet!!! AVOID IT when dry! DO NOT store! The purplish iodine vapor this produces during the explosion will stain and corrode!

- 1) Take a small plastic bucket, add 3-4 inches of household ammonia. This bucket will never be clean again, in all likelihood. Try to get clear (non-pine, non-cloudy) ammonia. Or use an ammonium hydroxide solution from a chemlab. This results in better but more sensitive, and therefore dangerous crystals.
- 2) Drop in iodine (like you use on scratches) one drop at a time, or, preferably, use crystals of iodine.
- 3) Let it settle, then pour it through a piece of cloth, discarding the runoff.
- 4) Squeeze *gently* to get out excess liquid.
- 5) Mold it onto the thing you want to blow up, stand **way** back.
- 6) Wait for it to dry, and throw a rock at it.

HOW TO BUILD A TENNIS BALL CANNON?

1. Get six (6) tin cans.
2. From five of them remove the tops and bottoms.
3. From the last one remove only the top. (this is the last can to make the breach)
4. The cans should overlap and be fit together to make a long barrel closed at one end and open at the other.



5. Duct tape all of the cans together. USE LOTS OF TAPE!!
6. Put some gunpowder in the bottom of the CANNON.
7. Aim, brace the CANNON.
8. Spray hairspray or pour alcohol on the tennis ball and light.
9. Drop the ball into the can and STAND BACK!

Other ideas:

- a) Make explosive tennis balls.
- b) Launch potatoes.
- c) Launch thumbtacks, nails, broken glass, etc.

