HACKING, INFULTRATION AND CIRCUIT DEACTIVATION.

Compiled by REDACTED

TOP SECRET

This document is for the eyes of those with "WHP"-level clearance only.

Delete this file immediately if you have insufficient clearance.

FORWARD

Hello.

I have been asked to create this document in order to support fellow agents, as well as my future self.

Phase 2 of the Sleeper Agent Initiative is inevitable, and I will soon forget this knowledge.

Hopefully, I will still possess these skills when I am activated. If not, this document should be most useful.

Good luck,
REDACTED

CONTENTS

I
THE ENHANCED TERMINAL

From your basic training you should be familiar with the Standard Terminal.

The Standard Terminal accepts 6-character inputs and it has limited use with high-level operations. Advanced infiltration techniques require access to the Enhanced Terminal.

To access the Enhance Terminal, type “launch” into the Standard Terminal.

The Enhanced Terminal accepts 8-character inputs.
Most inputs start with a 4-character command, followed by 4-characters of details.

For example,
The command “vrfy” followed by an agent’s 4-digit ID will return a verification code, useful for initiating encrypted communication.

II

CIRCUIT DEACTIVATION

The deactivation of electronical components is a vital skill for successful infiltration.

Circuits involve several wired connections. To deactivate a circuit one must cut a selection of connections whilst leaving vital connections intact.

Circuits are identified with a 4-character Circuit Code, with the first character being its series.

The vast majority of circuitry is of one of two types: **Y-series** or **Z-series**.

Circuit schematics can be researched using the "schm" command followed by the Circuit's Code.

The following page shows the details of which wires should be cut in order to deactivate a circuit.

Y-SERIES CIRCUIT

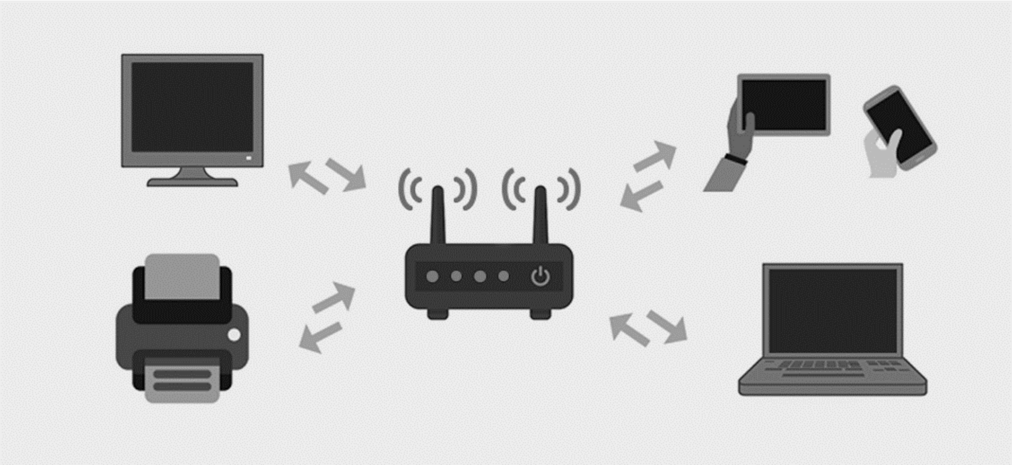
- Cut all Red wires.
- Only cut Blue wires where the top connection is larger than the bottom connection.
- Only Cut the Green wires when there is a vowel in the Circuit Code.

Z-SERIES CIRCUIT

- Cut all Green wires.
- Only cut Blue wires where the top connection is smaller than the bottom connection.
- Only Cut the Red wires when there is a vowel in the Circuit Code.

III

IDENTIFYING ADDRESSES



Having physical access to a target device is desirable but not always feasible. Being able to remotely access network-connected devices is of clear importance.

To be able to operate on these devices, their network address must be known.

For a multitude of reasons, these addresses may be hidden or obfuscated to those without strict credentials in the network. As a result, often only partial addresses are visible.

Address tables can be used to re-construct these partial addresses, allowing for device access and further infiltration.

Address Table

An Address Table can be accessed using the command "atbl" followed by the 4-character Partial Address.

Every Address Table provides a starting position [S], and an ending position [E]. One must traverse the table, moving orthogonally one cell each time.

You will append or prepend the Partial Address with the given character given in each cell.

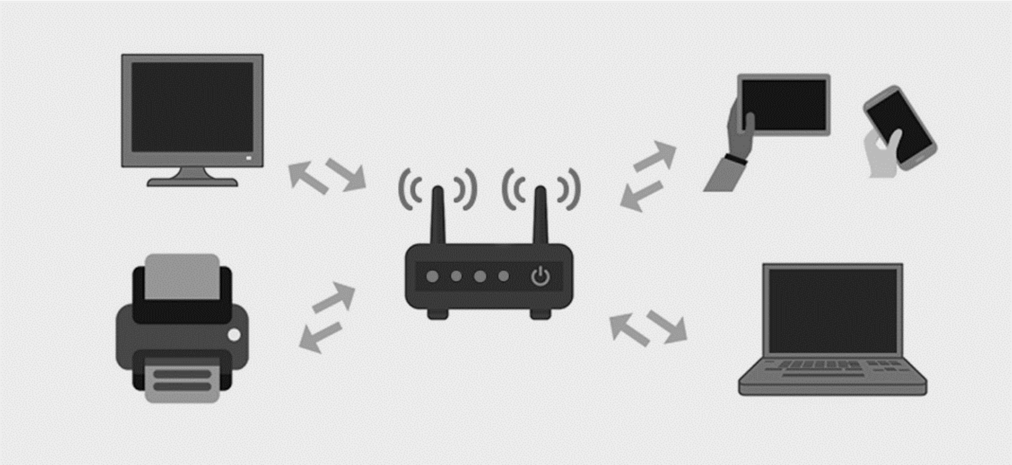
When multiple paths are available, the shortest should be chosen.

Notes

- "G_" means prepend the Partial Address with a "G".
- "_G" means append the Partial Address with a "G".
- "X" is not a valid Address character. The "_X" instruction means delete the last character of the Partial Address. Similarly, "X_" means delete the first.
- Most tables have unreachable tiles marked by "######". You cannot move onto these.
- Some tables have locked cells, marked by [L]. You must first pick up a key [K] in order to pass through these cells.
- All cells are activated once only. If they are moved onto a second time, no modification of the Partial Address is required.

IV

COMPROMISING CLUSTERS



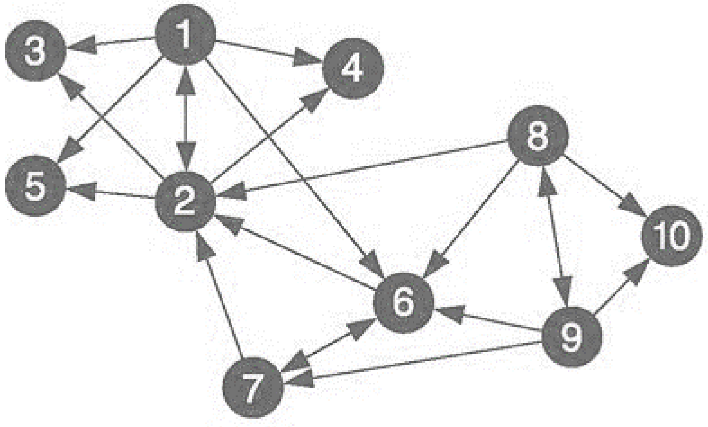
CLUSTERS & ENDPOINTS

A Cluster is a collection of Endpoints on a network.

An Endpoint is simply any device or server that has communications with a Cluster.

All Clusters have a 6-digit Cluster ID.
All Endpoints have a 4-digit Endpoint ID.

Clusters are often used for faster communication between Endpoints, and for security – as all Endpoints need to be compromised in order to compromise a Cluster.



COMPROMISING A CLUSTER

To compromise a Cluster, one must compromise all connected Endpoints and gain their Access Tokens.

These Access Tokens are then to be subtracted from the Cluster's ID.

Initiate a final hack with the command "hk" followed by the reduced Cluster ID. If successful, a PAYLOAD will be received.

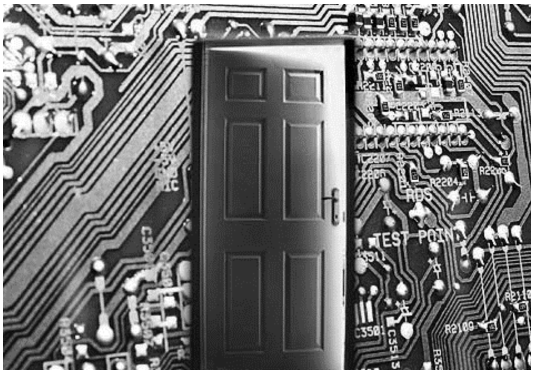
COMPROMISING ENDPOINTS

To scan for a Cluster's Endpoints, initiate a Cluster scan by using the command "cs" followed by the Cluster's ID.

Each Endpoint is likely to have some weakness. To establish the weakness of an Endpoint, use the command "wkns" followed by the Endpoint's ID.

The following pages discuss the various Endpoint vulnerabilities.

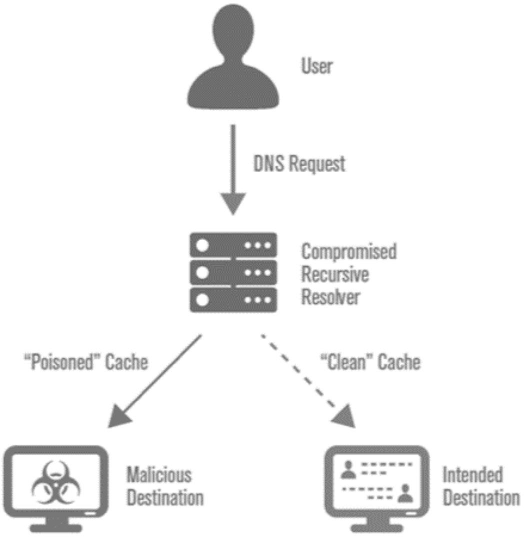
BACKDOOR WEAKNESS



Endpoints may already have a backdoor in place due to a prior breach, as an intentional feature for ease of employee access, or simply to appease REDACTED.

To access an Endpoint's backdoor, if it exists, type "bkdr" followed by the Endpoint's ID.

DNS CACHE WEAKNESS



An Endpoint's over-reliance on stored DNS information can be an excellent opportunity for temporary interception of network traffic.

This exploit involves spoofing the authorisation process of the Endpoint's DNS cache, and monitoring the incoming requests.

The command "auth" followed by the Authorisation Value (initially the Endpoint's ID) will allow progression through the process.

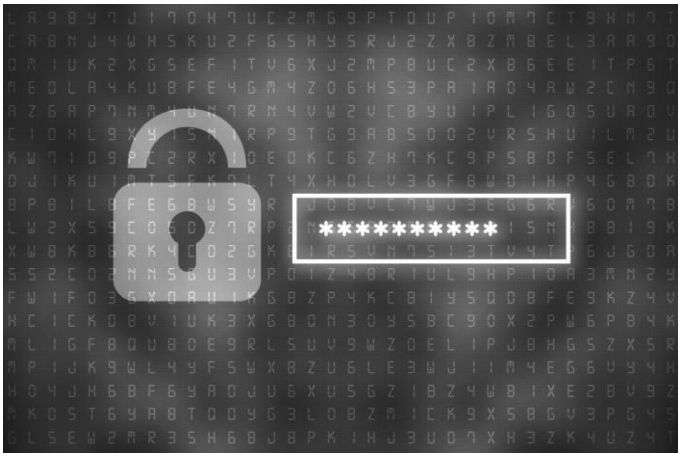
Modify this by taking note of the Request Operation and Request Number.
Continue to spoof the authorisation with the "auth" command followed by the modified Authorisation Value.

PASSWORD WEAKNESS

Occasionally Endpoints will be connected to networks before their passwords have been changed from their default.

The attack vector for this weakness is essentially brute forcing the default passwords.

Input a password by typing the Endpoint ID followed by the password.



Below is a list of possible default passwords for various Endpoint manufacturers.

- RedLink: ADMN, PASS, 1234, CHNG, RRRR, 2020
- PowerBlue: ADMN, P4SS, 4321, DEFT, BBBB, 2019
- EvergreenTech: ADMN, PSWD, 9876, NORM, EEEE, YEAR
- PurpleSolutions: ADMN, WORD, 6789, BASC, PPPP, TIME
- GreyServices: ADMN, TEMP, 5555, STRD, GGGG, MNTH

DATABASE WEAKNESS

Most database management systems release updates much more slowly than vulnerabilities are found.

Although exploits for these systems are often patched, they remain a valid basis for an attack on outdated Endpoints.

All attack vectors involve code-injection and modification of the databases' Release Number. To exploit a database weakness, use "injt" followed by the modified Release Number.

Below is a table of successful attack vectors for Release Number modification.

Main	Sub-	Attack Vector
3	7	NULL PASSWORD
3	8	BOOLEAN EVALUATION
3	9	CREDENTIAL SWITCH
4	0	QUERY ESCAPE

Database versions have the following structure:

A.B.CCCC

A = Main version number

B = Sub-version number

CCCC = Release number

Obtain the current database's version and other details by running "dbdt" followed by the Endpoint's ID.

DATABASE WEAKNESS

NULL PASSWORD

This exploit involves bypassing the database's password-verification procedure.

Modify the Release Number by replacing the first 2 digits with exclamation points (**!**) and the last 2 digits with the sum of the four original Release Number digits.

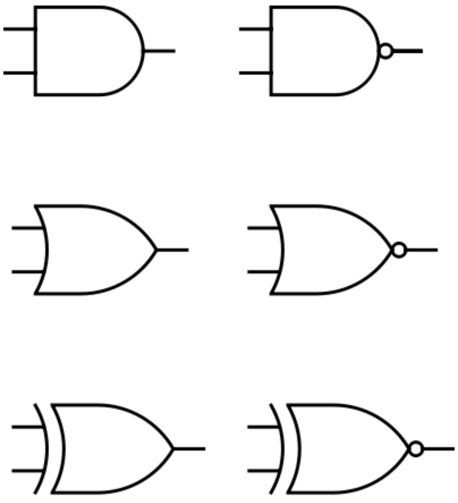
This exploit was fixed by a simple existence check on all user input.

BOOLEAN EVALUATION

This exploit provides the database with various objects that evaluate to True.

Modify the Release Number by replacing all even digits with "T" and all odd digits with "Y".

This exploit was fixed by a removal of input evaluation on users without valid credentials.



DATABASE WEAKNESS

CREDENTIAL SWITCH

This exploit centres around confusing the target Endpoint and switching its credentials with a connected user.

Modify the Release Number by switching the smallest digit with the largest digit.

This exploit was fixed by an extra user-verification step added in a future version.

QUERY ESCAPE

This exploit terminates a query before the databases' expectation, allowing for the user to initiate their own query.

Modify the Release Number by replacing the first and last digit with hyphens. (-).

This exploit has no current fix.

V

DECRYPTION

REDACTED

[redacted]

[redacted]

[redacted]

[redacted]

Editor note

Before publication, we drastically need to improve the encryption of our files.

For example, in many records agent data is encrypted with a simple
0 = A, 1 = B, …, 25 = Z system.