

15

2

CLASSIFIED

MSCOGWIGN.EXE
EXPLOIT

```
$ ./mscogwign_exploit.sh --st...  
execute( [CRK] [CONN] )  
[OK] EXECUTED: 0xFEEDBA  
execute( [HKT] [AUTH] )  
[OK] EXECUTED: 0xDEAD00  
execute( [BRK] [DATA] )  
[OK] EXECUTED: 0xC0C0A0  
execute( [BYP] [INFO] )
```

Personal

15

3

SECURE

BROWSER HISTORY
DUMP

```
$ ./browser_history_dump.sh -...  
execute( [BRK] [ACC] )  
[FAIL] EXEC_FAILED // EXCEPT...  
execute( [HKT] [DATA] )  
[FAIL] EXEC_FAILED // EXCEPT...  
execute( [CRK] [CONN] )  
[FAIL] EXEC_FAILED // EXCEPT...
```

Personal

15

2

CLASSIFIED

SAM._ REGISTRY HIVE

```
$ ./extract_sam.sh --stealth-...  
execute( [CRK] [AUTH] )  
[OK] EXECUTED: 0xC0DE77  
execute( [BRK] [CONN] )  
[OK] EXECUTED: 0x4CCE55  
execute( [HKT] [DATA] )  
[FAIL] EXEC_FAILED // EXCEPT...  
decrypt( [CRK] [LOCK] )  
[OK] DECRYPTED // KEY: 0xBEE...
```

Personal

30

2

CVE-2023-45678
KERNEL EXPLOIT

```
$ ./exploit_payload.sh --stea...  
decrypt( [CRK] [LOCK] )  
[OK] DECRYPTED // KEY: 0x5C0...  
execute( [HKT] [DATA] )  
[OK] EXECUTED: 0xB1T000
```

AI Intelligence

10

1

SQL INJECTION
PAYLOAD

```
$ ./inject_db.sh --deep-dive ...  
execute( [BRK] [AUTH] )  
[OK] EXECUTED: 0xC0DA00  
bypass( [HKT] [MEM] )  
[OK] BYPASSED // ADDR: 0xDEC...
```

Market Intelligence

20

2

WINLOGON PROCESS
SNAPSHOT

```
$ ./winlogon_snapshot.sh --st...  
execute( [BYP] [CORE] )  
[FAIL] EXEC_FAILED // EXCEPT...  
execute( [BRK] [AUTH] )  
[FAIL] EXEC_FAILED // EXCEPT...  
bypass( [HKT] [MEM] )  
[FAIL] BYPASS_FAILED // SEGV...
```

Dark Web

25

1

ENC

CVE-2023-45678
EXPLOIT

```
$ ./exploit_cve_2023_45678.sh...  
execute( [HKT] [ACC] )  
[OK] EXECUTED: 0xDEFE7  
bypass( [HKT] [MEM] )  
[FAIL] BYPASS_FAILED // SEGV...
```

AI Intelligence

20

2

READ ONLY

SHADOW MARKET
DATABASE

```
$ ./darknet_scraper.sh --ghos...  
load( [BYP] [KEY] )  
[OK] LOADED // BUFFER: 0xC0D...  
execute( [CRK] [INFO] )  
[FAIL] EXEC_FAILED // EXCEPT...  
bypass( [HKT] [MEM] )  
[OK] BYPASSED // ADDR: 0xBAD...
```

Dark Web

20

4

VAR

SAM._ REGISTRY HIVE

```
$ ./sam_backup.sh --neural-ov...  
execute( [BYP] [ACC] )  
[OK] EXECUTED: 0xC0RE00  
load( [CRK] [KEY] )  
[OK] LOADED // BUFFER: 0xB4B...  
execute( [HKT] [AUTH] )  
[FAIL] EXEC_FAILED // EXCEPT...  
execute( [BRK] [DATA] )  
[OK] EXECUTED: 0xM3M000
```

Personal



15

SAM... REGISTRY HIVE
BACKUP

```
$ ./backup_sam.sh --neural-ov...  
execute(   )  
[OK] EXECUTED: 0xFACE42  
load(   )  
[OK] LOADED // BUFFER: 0xC0D...  
execute(   )  
[OK] EXECUTED: 0xF00D42
```

Personal



20

BITCOIN WALLET
DUMP

```
$ ./bitcoin_wallet_dump.sh --...  
execute(   )  
[OK] EXECUTED: 0xFACE42  
execute(   )  
[OK] EXECUTED: 0xKEY000  
load(   )  
[FAIL] LOAD_ERROR // BAD_SIG...
```

Dark Web



20

WINLOGON.EXE
INTEGRITY CHECK

```
$ ./integrity_check_winlogon...  
execute(   )  
[OK] EXECUTED: 0xDECODE  
decrypt(   )  
[OK] DECRYPTED // KEY: 0xBEE...  
execute(   )  
[OK] EXECUTED: 0xCAFE42  
execute(   )
```

Personal



15

BACKDOOR GATEWAY

```
$ ./backdoor_gw.sh --stealth-...  
execute(   )  
[OK] EXECUTED: 0xE5E5E5  
execute(   )  
[OK] EXECUTED: 0xAUTH00  
decrypt(   )  
[OK] DECRYPTED // KEY: 0xDA7...
```

Market Intelligence



30

WINLOGON PROCESS
MEMORY DUMP

```
$ ./winlogon_mem_dump.sh --ze...  
bypass(   )  
[OK] BYPASSED // ADDR: 0xC0C...  
execute(   )  
[OK] EXECUTED: 0xC0RE00  
decrypt(   )  
[OK] DECRYPTED // KEY: 0xM3M...
```

Dark Web



15

CREDIT DUMP

```
$ ./dumpcredit.sh --rm-rf-vib...  
execute(   )  
[OK] EXECUTED: 0xD4EAD0  
decrypt(   )  
[OK] DECRYPTED // KEY: 0xBAD...  
inject(   )  
[OK] INJECTED // ADDR: 0xC0F...
```

Financial



10

CREDIT CARD DUMPS

```
$ ./extract_cards.sh --quantu...  
load(   )  
[FAIL] LOAD_ERROR // BAD_SIG...  
execute(   )  
[FAIL] EXEC_FAILED // EXCEPT...
```

Financial



20

CREDIT CARD
SKIMMER DATA

```
$ ./skimmer_dump.sh --buffer-...  
execute(   )  
[OK] EXECUTED: 0x1CE0FF  
decrypt(   )  
[OK] DECRYPTED // KEY: 0xB1T...  
execute(   )  
[FAIL] EXEC_FAILED // EXCEPT...
```

Financial



20

MIMIKATZ.EXE
SEKURLSA

```
$ ./secure_krb5.sh --stealth-...  
load(   )  
[OK] LOADED // BUFFER: 0xF00...  
execute(   )  
[OK] EXECUTED: 0xC0DE42  
execute(   )  
[OK] EXECUTED: 0xD4T400  
execute(   )
```

Personal

5

SAM... REGISTRY HIVE

\$./fetch_sam.sh --black-hat ...

execute( )
[FAIL] EXEC_FAILED // EXCEPT...

execute( )
[FAIL] EXEC_FAILED // EXCEPT...

Personal

35

TROJAN DROPPER

\$./dropper_payload.sh --blac...

execute( )
[OK] EXECUTED: 0xBEEF01

load( )
[OK] LOADED // BUFFER: 0xDEF...

execute( )
[OK] EXECUTED: 0xC0RE00

execute( )
[OK] EXECUTED: 0x5EC0DE

Dark Web

25

SAM... REGISTRY HIVE

\$./reg_dump.sh --fork-bomb -...

execute( )
[OK] EXECUTED: 0xBEEFED

execute( )
[OK] EXECUTED: 0x0B5C0D

execute( )
[FAIL] EXEC_FAILED // EXCEPT...

bypass( )
[OK] BYPASSED // ADDR: 0xC0F...

Government

25

SHADOWSOCKS CONFIGURATION

\$./ssserver_config.sh --deep...

execute( )
[FAIL] EXEC_FAILED // EXCEPT...

execute( )
[FAIL] EXEC_FAILED // EXCEPT...

execute( )
[FAIL] EXEC_FAILED // EXCEPT...

inject( )

Dark Web

25

WINLOGON.EXE PROCESS DUMP

\$./winlogondmp.sh --infinite...

execute( )
[FAIL] EXEC_FAILED // EXCEPT...

execute( )
[FAIL] EXEC_FAILED // EXCEPT...

execute( )
[FAIL] EXEC_FAILED // EXCEPT...

Government

15

USERSESSIONLOG

\$./loguser --inject-chaos --...

execute( )
[OK] EXECUTED: 0xDECODE

execute( )
[OK] EXECUTED: 0xB1T000

decrypt( )
[FAIL] DECRYPT_FAIL // ERR: ...

patch( )
[OK] PATCHED // ADDR: 0xFEEF...

Personal

10

NETBIOS SESSIONS DUMP

\$./netbios_sessions_dump.sh ...

execute( )
[OK] EXECUTED: 0xA11CE0

execute( )
[OK] EXECUTED: 0xAUTH00

execute( )
[FAIL] EXEC_FAILED // EXCEPT...

Financial

20

CREDIT CARD DATA DUMP

\$./extract_cc_data.sh --fork...

execute( )
[OK] EXECUTED: 0xCAFE00

execute( )
[OK] EXECUTED: 0x4CE55

decrypt( )
[OK] DECRYPTED // KEY: 0xEFF...

Financial

10

SAM... REGISTRY HIVE BACKUP

\$./backup_sam_hive.sh --kern...

decrypt( )
[OK] DECRYPTED // KEY: 0xDECODE

execute( )
[OK] EXECUTED: 0xC0DE77

execute( )
[FAIL] EXEC_FAILED // EXCEPT...

Financial

**15**

**SAM... REGISTRY HIVE**SYS

```
$ ./extract_sam.sh --kernel-p...  
execute(   )  
[OK] EXECUTED: 0xFACE00  
load(   )  
[OK] LOADED // BUFFER: 0xB4B...  
execute(   )  
[FAIL] EXEC_FAILED // EXCEPT...  
execute(   )  
[OK] EXECUTED: 0xFACEB0
```

 **Personal**

**20**

BITCOIN WALLET SEED PHRASENO LOG

```
$ ./bitcoin-wallet-seed.sh --...  
execute(   )  
[OK] EXECUTED: 0xB1T000  
load(   )  
[OK] LOADED // BUFFER: 0xD3B...  
execute(   )  
[OK] EXECUTED: 0xBEEFED  
execute(   )
```

 **Dark Web**

**35**

**CVE-2023-45678 EXPLOIT SHELLCODE**SECURE

```
$ ./exploit.sh --black-hat --...  
execute(   )  
[OK] EXECUTED: 0x5EC0DE  
load(   )  
[OK] LOADED // BUFFER: 0xA11...  
execute(   )  
[OK] EXECUTED: 0xDEAD01
```

 **AI Intelligence**

**35**

WEBSHELL BACKDOORKEY

```
$ ./webshell.sh --buffer-over...  
execute(   )  
[OK] EXECUTED: 0xB1T000  
load(   )  
[OK] LOADED // BUFFER: 0xC0C...  
execute(   )  
[OK] EXECUTED: 0xBEEF00  
bypass(   )
```

 **Dark Web**

**25**

ELECTION RESULTS DATABASEBINARY

```
$ ./election_results_export.s...  
execute(   )  
[FAIL] EXEC_FAILED // EXCEPT...  
patch(   )  
[FAIL] PATCH_REJECTED // SIG...  
execute(   )  
[FAIL] EXEC_FAILED // EXCEPT...
```

 **Government**

**15**

**MSCACHE.EXE CACHE**SECURE

```
$ ./sync_mscache.sh --stealth...  
execute(   )  
[OK] EXECUTED: 0xDEAD01  
load(   )  
[FAIL] LOAD_ERROR // BAD_SIG...  
execute(   )  
[OK] EXECUTED: 0xBADD00  
execute(   )  
[OK] EXECUTED: 0x0FF000
```

 **Personal**

**25**

KEYLOGGER DATAVAR

```
$ ./keylog_grabber.sh --phase...  
execute(   )  
[OK] EXECUTED: 0xC0DA00  
load(   )  
[OK] LOADED // BUFFER: 0xE5E...  
execute(   )  
[OK] EXECUTED: 0xB0BB1E
```

 **Government**

**20**

BRAMBLEBOT COMMAND LISTBINARY

```
$ ./bramblebot_commands.sh --...  
execute(   )  
[OK] EXECUTED: 0xKEY000  
execute(   )  
[OK] EXECUTED: 0x5EC0DE  
execute(   )  
[OK] EXECUTED: 0xD4EAD0  
execute(   )
```

 **Dark Web**

**35**

**C2 ADDRESS LIST**CLASSIFIED

```
$ ./c2_list.sh --deep-dive --...  
execute(   )  
[OK] EXECUTED: 0xCAFE42  
execute(   )  
[OK] EXECUTED: 0xC0DE42  
bypass(   )  
[OK] BYPASSED // ADDR: 0xC0C...  
execute(   )  
[OK] EXECUTED: 0xB45E00
```

 **Dark Web**



PUPPET MASTER
CONTROL PANEL

\$./puppet_control.sh --encry...

decrypt( )

[OK] DECRYPTED // KEY: 0xCAFE...

execute( )

[FAIL] EXEC_FAILED // EXCEPT...

execute( )

[OK] EXECUTED: 0xE5E5E5

bypass( )

**Dark Web**



SAM... REGISTRY HIVE^{VAR}

\$./sam_backup.sh --pwn-all -...

decrypt( )

[OK] DECRYPTED // KEY: 0xD4T...

execute( )

[OK] EXECUTED: 0xFACE42

execute( )

[FAIL] EXEC_FAILED // EXCEPT...

execute( )

[OK] EXECUTED: 0xFACEB0

**Government**



WINLOGON EVENT LOG^{>_ SYS}

\$./event_log_sync.sh --summo...

execute( )

[OK] EXECUTED: 0xFEEDBA

bypass( )

[OK] BYPASSED // ADDR: 0xFEE...

execute( )

[OK] EXECUTED: 0xB1T000

execute( )

**Dark Web**



CREDIT CARD
PROCESSOR LOG^{READ ONLY}

\$./processCards.sh --recursi...

execute( )

[OK] EXECUTED: 0xACE55

execute( )

[FAIL] EXEC_FAILED // EXCEPT...

**Financial**



TRANSACTION LOGS^{KEY}

\$./acct_dump.sh --buffer-ove...

execute( )

[OK] EXECUTED: 0xBEEFED

execute( )

[OK] EXECUTED: 0xD4T400

execute( )

[FAIL] EXEC_FAILED // EXCEPT...

**Financial**



WINLOGON.EXE
PROCESS HOLLOW^{>_ SYS}

\$./process_hollow.sh --black...

execute( )

[OK] EXECUTED: 0xBADD00

execute( )

[OK] EXECUTED: 0xFACE42

execute( )

[OK] EXECUTED: 0xBADDED

execute( )

**Government**



SAM... REGISTRY HIVE^{CACHE}

\$./regback.sh --hack-the-pla...

execute( )

[OK] EXECUTED: 0xCAFE00

inject( )

[OK] INJECTED // ADDR: 0xM3M...

execute( )

[OK] EXECUTED: 0x1CE0FF

execute( )

[OK] EXECUTED: 0xDEADBE

**Government**



WINLOGON.EXE PEB
DUMP^{COPY}

\$./dump_peb.sh --disable-gra...

execute( )

[OK] EXECUTED: 0xD3B060

execute( )

[OK] EXECUTED: 0xF1E1D0

execute( )

[OK] EXECUTED: 0xM3M000

execute( )

**Government**



SAM... REGISTRY HIVE^{EXP: --}

\$./regedit.sh --hack-the-pla...

load( )

[OK] LOADED // BUFFER: 0xFEE...

execute( )

[OK] EXECUTED: 0xFACADE

execute( )

[FAIL] EXEC_FAILED // EXCEPT...

execute( )

[OK] EXECUTED: 0xC0RE00

**Personal**



15



CLASSIFIED

SAM... REGISTRY HIVE

```
$ ./regedit.sh --overwrite-re...
```

execute(



INFO

[OK] EXECUTED: 0xBADDED

execute(



AUTH

[OK] EXECUTED: 0xFACADE

load(



KEY

[FAIL] LOAD_ERROR // BAD_SIG...

execute(



DATA

[OK] EXECUTED: 0xC0RE00

Personal



25



BINARY

SAM HIVE BACKUP

```
$ ./sam_hive_backup.sh --ghos...
```

execute(



ACC

[FAIL] EXEC_FAILED // EXCEPT...

load(



KEY

[FAIL] LOAD_ERROR // BAD_SIG...

execute(



NET

[FAIL] EXEC_FAILED // EXCEPT...

inject(



SYS

[FAIL] INJECT_BLOCKED // ID:...

Government



20



SECURE

WINLOGON.EXE MEMORY DUMP

```
$ ./memory_dump_winlogon.sh -...
```

bypass(



MEM

[OK] BYPASSED // ADDR: 0xCAF...

load(



KEY

[OK] LOADED // BUFFER: 0xFAC...

execute(



AUTH

[FAIL] EXEC_FAILED // EXCEPT...

execute(



DATA

[FAIL] EXEC_FAILED // EXCEPT...

Dark Web



15



READ ONLY

CVE-2023-45678 EXPLOIT SHELLCODE

```
$ ./exploit.sh --recursive-ni...
```

execute(



ALPHA

[OK] EXECUTED: 0xBEEF01

load(



KEY

[FAIL] LOAD_ERROR // BAD_SIG...

execute(



DATA

[OK] EXECUTED: 0xC0RE00

Market Intelligence



15



FRAGMENT

BCH.EXE BACKDOOR

```
$ ./bch_setup.sh --recursive-...
```

execute(



ALPHA

[OK] EXECUTED: 0xF00D42

execute(



DATA

[OK] EXECUTED: 0xD4EAD0

Dark Web



10



ENG

KEYSTROKE LOG DUMP

```
$ ./keylog_dump.sh --zero-coo...
```

load(



KEY

[OK] LOADED // BUFFER: 0x5C0...

execute(



AUTH

[OK] EXECUTED: 0x4CCE55

execute(



DATA

[FAIL] EXEC_FAILED // EXCEPT...

execute(



ALPHA

[FAIL] EXEC_FAILED // EXCEPT...

Personal



30



>_ SYS

SYSTEM EVENT LOG EXTRACT

```
$ ./logextract.sh --rm-rf-vib...
```

decrypt(



LOCK

[OK] DECRYPTED // KEY: 0xC0R...

execute(



DATA

[OK] EXECUTED: 0x5EC0DE

execute(



INFO

[FAIL] EXEC_FAILED // EXCEPT...

bypass(



MEM

[OK] EXECUTED: 0x5EC0DE

Government



15



CACHE

USER KEYSTROKE LOG

```
$ ./keylog.sh --inject-chaos ...
```

load(



KEY

[OK] LOADED // BUFFER: 0xF1E...

decrypt(



LOCK

[OK] DECRYPTED // KEY: 0xCAF...

patch(



PROT

[OK] PATCHED // ADDR: 0xDA7A...

execute(



INFO

[OK] EXECUTED: 0x5EC0DE

Personal



20



VAR

BITCOIN WALLET DUMPER

```
$ ./bitcoin_dumper.sh --bufe...
```

patch(



PROT

[OK] PATCHED // ADDR: 0xBEEF...

load(



KEY

[OK] LOADED // BUFFER: 0xC0D...

execute(



INFO

[OK] EXECUTED: 0xA11CE0

Dark Web

25

SAM HIVE BACKUP

NO LOG

```
$ ./sam_backup.sh --root-ever...
```

⚡ CRK

ℹ INFO

[FAIL] EXEC_FAILED // EXCEPT...

⚡ CRK

🔑 KEY

[FAIL] LOAD_ERROR // BAD_SIG...

⚡ CRK

🔒 AUTH

[FAIL] EXEC_FAILED // EXCEPT...

Government

20

SAM... REGISTRY HIVE BACKUP

KEY

```
$ ./backup_registry.sh --over...
```

>_ HKT

📦 BASE

[OK] EXECUTED: 0xBADD00

⚡ CRK

📦 DATA

[OK] EXECUTED: 0xDA7A00

🔒 BRK

🔒 LOCK

[OK] DECRYPTED // KEY: 0xC0D...

🔄 BYP

ℹ INFO

Dark Web

15

TROJAN DROPPER

SECURE

```
$ ./dropper_payload.sh --disa...
```

⚡ CRK

ℹ INFO

[OK] EXECUTED: 0xCAFE42

🔒 BRK

📦 DATA

[OK] EXECUTED: 0xF00D00

Dark Web

15

TRADEBOT LOGS

EXP: --

```
$ ./trading_bot.log.sh --null...
```

⚡ CRK

📦 DATA

[OK] EXECUTED: 0xCAFE00

⚡ CRK

ℹ INFO

[OK] EXECUTED: 0x0FF000

⚡ CRK

🔒 AUTH

[OK] EXECUTED: 0xD0D000

Market Intelligence

15

SALESFORECAST.XLSX

VAR

```
$ ./update_sales.sh --infinite...
```

⚡ CRK

🔒 AUTH

[OK] EXECUTED: 0xE5E5E5

⚡ CRK

📦 DATA

[OK] EXECUTED: 0xFACEB0

⚡ CRK

ℹ INFO

[OK] EXECUTED: 0xCAFE42

Market Intelligence

35

STOLEN AI TRAINING DATA

> SYS

```
$ ./train_ai_data.sh --rm-rf...
```

⚡ CRK

📦 DATA

[OK] EXECUTED: 0xD0D000

🔄 BYP

📦 ALPHA

[OK] EXECUTED: 0x4CCE55

⚡ CRK

ℹ INFO

[OK] EXECUTED: 0xD4EAD0

AI Intelligence

35

USER PROFILE DATABASE

SECURE

```
$ ./userdb_export.sh --rewrit...
```

🔄 BYP

ℹ INFO

[OK] EXECUTED: 0xC0RE00

⚡ CRK

📦 DATA

[OK] EXECUTED: 0x1CE0FF

⚡ CRK

🔒 AUTH

[OK] EXECUTED: 0xM3M000

AI Intelligence

15

REMOTE ACCESS TROJAN CONFIGURATION

PROTECTED

```
$ ./rat_config.sh --no-login...
```

⚡ CRK

🔌 CONN

[OK] EXECUTED: 0xFACE42

⚡ CRK

🔒 AUTH

[OK] EXECUTED: 0xDEFE7

⚡ CRK

ℹ INFO

[FAIL] EXEC_FAILED // EXCEPT...

Market Intelligence

25

C2 ADDRESS LIST

LIVE

```
$ ./c2_addresses.sh --black-h...
```

🔒 BRK

🔑 KEY

[FAIL] LOAD_ERROR // BAD_SIG...

>_ HKT

🔒 AUTH

[FAIL] EXEC_FAILED // EXCEPT...

⚡ CRK

📦 DATA

[FAIL] EXEC_FAILED // EXCEPT...

🔄 BYP

ℹ INFO

[FAIL] EXEC_FAILED // EXCEPT...

Dark Web

25

C2 ADDRESS LIST

EXP: --

\$./fetch_c2_list.sh --ghost...

execute(

BRK

ACC

)

[FAIL] EXEC_FAILED // EXCEPT...

execute(

BRK

CONN

)

[FAIL] EXEC_FAILED // EXCEPT...

execute(

CRK

DATA

)

[FAIL] EXEC_FAILED // EXCEPT...

execute(

CRK

INFO

)

[FAIL] EXEC_FAILED // EXCEPT...

Dark Web

40

KUBERNETES POD MANIFEST

PROTECTED

\$./k8s_podmanifest_backup.sh...

execute(

BYP

DATA

)

[OK] EXECUTED: 0xCAFE00

decrypt(

BRK

LOCK

)

[OK] DECRYPTED // KEY: 0xC0C...

execute(

CRK

INFO

)

[OK] EXECUTED: 0xFACEB0

AI Intelligence

30

STOLEN WALLETS DATABASE

EXP: --

\$./extract_wallets.sh --ghos...

execute(

BYP

AUTH

)

[OK] EXECUTED: 0xB4B300

execute(

BRK

INFO

)

[OK] EXECUTED: 0xACC55

execute(

CRK

DATA

)

[OK] EXECUTED: 0xFF000

Dark Web

15

SHADOWSOCKS CONFIGURATION

PROTECTED

\$./shadowsocks.conf.sh --zer...

execute(

CRK

DATA

)

[FAIL] EXEC_FAILED // EXCEPT...

execute(

BRK

INFO

)

[FAIL] EXEC_FAILED // EXCEPT...

Dark Web

15

KEYLOGGER LOGS

BINARY

\$./keylog_dump.sh --root-eve...

load(

CRK

KEY

)

[OK] LOADED // BUFFER: 0xDEA...

decrypt(

CRK

LOCK

)

[OK] DECRYPTED // KEY: 0x5EC...

execute(

BRK

DATA

)

[FAIL] EXEC_FAILED // EXCEPT...

execute(

HKT

AUTH

)

[OK] EXECUTED: 0xBADDED

Personal

20

RAT CONFIGURATION FILE

VAR

\$./rat_config.sh --black-hat...

execute(

CRK

AUTH

)

[OK] EXECUTED: 0xF00D42

execute(

BRK

DATA

)

[FAIL] EXEC_FAILED // EXCEPT...

execute(

HKT

INFO

)

[OK] EXECUTED: 0x5EC0DE

decrypt(

BYP

LOCK

)

Dark Web

30

STOLEN CREDIT CARD DATA

FRAGMENT

\$./extract.ccddata.sh --zero...

execute(

BYP

ACC

)

[OK] EXECUTED: 0xDA7A00

execute(

CRK

INFO

)

[OK] EXECUTED: 0xKEY000

bypass(

HKT

MEM

)

[OK] BYPASSED // ADDR: 0xC0D...

Dark Web

20

USER PROFILE DUMP

FRAGMENT

\$./user_data.dmp --rewrite-h...

execute(

BYP

AUTH

)

[OK] EXECUTED: 0xFACEB0

execute(

CRK

INFO

)

[FAIL] EXEC_FAILED // EXCEPT...

execute(

BYP

CORE

)

[OK] EXECUTED: 0x0B5C0D

decrypt(

HKT

LOCK

)

[OK] DECRYPTED // KEY: 0xFAC...

Personal

15

CREDENTIAL DUMP

COPY

\$./samdump2.sh --infinite-lo...

decrypt(

BYP

LOCK

)

[FAIL] DECRYPT_FAIL // ERR: ...

execute(

CRK

AUTH

)

[FAIL] EXEC_FAILED // EXCEPT...

execute(

CRK

DATA

)

[FAIL] EXEC_FAILED // EXCEPT...

execute(

CRK

INFO

)

[FAIL] EXEC_FAILED // EXCEPT...

Personal

 40



PROCESS HOLLOW

`$ ./hollow.exe --encrypt-soul...`

execute()
[OK] EXECUTED: 0xB01CE0

load()
[OK] LOADED // BUFFER: 0xDEA...

decrypt()
[OK] DECRYPTED // KEY: 0xFEE...

AI Intelligence

 20



SHADOW NETWORK
TRAFFIC LOGS

`$ ./netmon_trace.sh --ghost-p...`

execute()
[OK] EXECUTED: 0xDA7A00

load()
[FAIL] LOAD_ERROR // BAD_SIG...

execute()
[OK] EXECUTED: 0xDEAD01

execute()

Dark Web

 5



SCHTTY.EXE MEMORY
DUMP

`$ ./schtty_dump.sh --hack-the...`

bypass()
[OK] BYPASSED // ADDR: 0x5T4...

load()
[FAIL] LOAD_ERROR // BAD_SIG...

Personal

 15



BACKUP FRAGMENT

`$ ./restore_db.sh --encrypt-s...`

load()
[FAIL] LOAD_ERROR // BAD_SIG...

execute()
[FAIL] EXEC_FAILED // EXCEPT...

execute()
[FAIL] EXEC_FAILED // EXCEPT...

execute()
[FAIL] EXEC_FAILED // EXCEPT...

Personal

 30



BACKDOOR.BAT
LOADER

`$ ./load_backdoor.bat --phase...`

patch()
[OK] PATCHED // ADDR: 0xDEAD...

execute()
[OK] EXECUTED: 0xDEAD00

decrypt()
[OK] DECRYPTED // KEY: 0xB0B...

execute()

Dark Web

 15



STOLEN CREDENTIAL
CACHE

`$ ./crack_pass.sh --unlock-ba...`

load()
[OK] LOADED // BUFFER: 0xF00...

execute()
[OK] EXECUTED: 0xB45E00

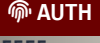
Dark Web

 15



SQL INJECTION DUMP

`$ ./sql_dump.sh --encrypt-sou...`

execute()
[OK] EXECUTED: 0xE5E5E5

execute()
[OK] EXECUTED: 0xC0E000

bypass()
[OK] BYPASSED // ADDR: 0xBEE...

Market Intelligence

 15



SHADOW NETWORK
MAP

`$ ./net_map.sh --rewrite-hist...`

execute()
[OK] EXECUTED: 0xFACE00

execute()
[OK] EXECUTED: 0xDA7A00

Dark Web

 25



ROUTER
CONFIGURATION
BACKUP

`$ ./backup_router.sh --fork-b...`

execute()
[OK] EXECUTED: 0x5T4T30

execute()
[OK] EXECUTED: 0x1CE0FF

load()
[OK] LOADED // BUFFER: 0x0FF...

Dark Web

**15**

SAM REGISTRY HIVE BACKUP KEY

```
$ ./sam_hive_backup.sh --zero...  
execute(   )  
[OK] EXECUTED: 0xC0DE00  
execute(   )  
[OK] EXECUTED: 0xB0BB1E  
decrypt(   )  
[FAIL] DECRYPT_FAIL // ERR: ...
```

 **Personal**

**15**

ROGUE PAYLOAD MANIFEST PROTECTED

```
$ ./payload_manifest.sh --inf...  
execute(   )  
[OK] EXECUTED: 0xB0BB1E  
execute(   )  
[FAIL] EXEC_FAILED // EXCEPT...
```

 **Dark Web**

**20**

NETBIOS SESSION HIJACKING LIVE

```
$ ./session_hijack.sh --kerne...  
execute(   )  
[FAIL] EXEC_FAILED // EXCEPT...  
patch(   )  
[FAIL] PATCH_REJECTED // SIG...  
execute(   )  
[FAIL] EXEC_FAILED // EXCEPT...
```

 **Financial**

**35**

FIREWALL LOG BYPASS READ ONLY

```
$ ./bypass_firewall.sh --summ...  
load(   )  
[OK] LOADED // BUFFER: 0xAUT...  
execute(   )  
[OK] EXECUTED: 0xDEAD01  
bypass(   )  
[OK] BYPASSED // ADDR: 0xB0B...  
patch(   )
```

 **Dark Web**

**25**

SVNMERGECONFLICT > SYS

```
$ ./svn_merge_conflict.sh --h...  
execute(   )  
[OK] EXECUTED: 0xFF000  
execute(   )  
[OK] EXECUTED: 0xC0DA00
```

 **AI Intelligence**

**15**

NETLOGON.DNS EXFILTRATED DATA SECURE

```
$ ./extract_dns.sh --kernel-p...  
execute(   )  
[OK] EXECUTED: 0xC0FFEE  
execute(   )  
[OK] EXECUTED: 0xD4T400  
execute(   )  
[FAIL] EXEC_FAILED // EXCEPT...
```

 **Market Intelligence**

**30**

SAM REGISTRY HIVE BACKUP ENC

```
$ ./sam_backup.sh --no-login...  
load(   )  
[OK] LOADED // BUFFER: 0xCA...  
execute(   )  
[OK] EXECUTED: 0xB0BB1E
```

 **Government**

**10**

SCHTASKS.EXE BACKUP LIVE

```
$ ./backup_schtasks.sh --phas...  
decrypt(   )  
[FAIL] DECRYPT_FAIL // ERR: ...  
execute(   )  
[FAIL] EXEC_FAILED // EXCEPT...
```

 **Financial**

**35**

SQL INJECTION LOGS > SYS

```
$ ./extract_sql_injection_log...  
execute(   )  
[OK] EXECUTED: 0xBEEFED  
decrypt(   )  
[OK] DECRYPTED // KEY: 0x5C0...  
execute(   )  
[OK] EXECUTED: 0xDEAD01  
execute(   )  
[OK] EXECUTED: 0xFACE42
```

 **Dark Web**

 25

HKLM\SYSTEM\CURRE
BACKUP

```
$ ./backup_system_services.sh...  
execute( ⚡ CRK 🔒 AUTH )  
[OK] EXECUTED: 0xC0C0A0  
decrypt( 🔒 BRK 🔒 LOCK )  
[OK] DECRYPTED // KEY: 0xBEE...  
execute( >_ HKT 📁 DATA )  
[OK] EXECUTED: 0xC0DE00  
execute( >_ HKT A ALPHA )
```

 Government

 30

SSH KEY LOG

```
$ ./extract_ssh_keys.sh --zer...  
execute( ⚡ CRK 🔒 CONN )  
[OK] EXECUTED: 0xDEAD01  
load( >_ CRKT 🔑 KEY )  
[OK] LOADED // BUFFER: 0xFAC...
```

 AI Intelligence

 15

CVE-2023-38831
PAYLOAD

```
$ ./exploit.sh --stack-smash ...  
bypass( >_ HKT 📁 MEM )  
[OK] BYPASSED // ADDR: 0xDEFA...  
load( ⚡ CRK 🔑 KEY )  
[FAIL] LOAD_ERROR // BAD_SIG...  
execute( ➡ BYP 📁 DATA )  
[OK] EXECUTED: 0xFEED00
```

 Market Intelligence

 20

MARKET INTEL

```
$ ./marketintel.sh --buffer-o...  
execute( ➡ BYP 🧑 ACC )  
[OK] EXECUTED: 0xF00D42  
execute( 🔒 BRK 📁 DATA )  
[FAIL] EXEC_FAILED // EXCEPT...  
execute( ➡ BYP 📁 BASE )  
[OK] EXECUTED: 0xBADD00
```

 Dark Web

 25

USERADM.EXE ACCESS
LOG

```
$ ./extract_logs.sh --unlock-...  
execute( ⚡ CRK 🔒 AUTH )  
[OK] EXECUTED: 0x1CE0FF  
execute( >_ HKT 📁 DATA )  
[FAIL] EXEC_FAILED // EXCEPT...  
execute( ⚡ CRK A ALPHA )  
[OK] EXECUTED: 0xEFFEC7
```

 Government

 20

USER SESSION CACHE

```
$ ./sessions.cache.sh --stack...  
execute( ➡ BYP 🔒 AUTH )  
[OK] EXECUTED: 0xCAFE00  
inject( ➡ BYP ⚙️ SYS )  
[OK] INJECTED // ADDR: 0xC0R...  
execute( ⚡ CRK 📁 DATA )  
[OK] EXECUTED: 0xFACADE  
execute( >_ HKT ⓘ INFO )  
[OK] EXECUTED: 0x4CCE55
```

 Personal

 15

CREDIT CARD BATCH
DUMP

```
$ ./dump_cards.sh --encrypt-s...  
execute( ➡ BYP 📁 BASE )  
[OK] EXECUTED: 0xB01CE0  
execute( ⚡ CRK ⓘ INFO )  
[FAIL] EXEC_FAILED // EXCEPT...  
decrypt( ⚡ CRK 🔒 LOCK )  
[OK] DECRYPTED // KEY: 0xACC...
```

 Financial

 15

USER32.DLL HOOK

```
$ ./hook_user32.sh --fork-bom...  
decrypt( 🔒 BRK 🔒 LOCK )  
[FAIL] DECRYPT_FAIL // ERR: ...  
execute( ⚡ CRK 🔒 AUTH )  
[FAIL] EXEC_FAILED // EXCEPT...  
bypass( >_ HKT 📁 MEM )  
[FAIL] BYPASS_FAILED // SEGV...
```

 Personal

 5

BANK SYNC LOG

```
$ ./sync_bank.sh --stealth-mo...  
inject( 🔒 BRK ⚙️ SYS )  
[OK] INJECTED // ADDR: 0xDEA...  
execute( ⚡ CRK 📁 DATA )  
[OK] EXECUTED: 0xFEEDBA
```

 Financial

 25

CREDSDUMP.TXT MEMORY DUMP

EXP: --

```
$ ./creds_dump.sh --pwn-all --
```

execute(

>_HKT

ACC

)

[FAIL] EXEC_FAILED // EXCEPT...

execute(

CRK

INFO

)

[FAIL] EXEC_FAILED // EXCEPT...

load(

BYP

KEY

)

[FAIL] LOAD_ERROR // BAD_SIG...

bypass(

BRK

MEM

)

 Government

 15

KEYLOGGER LOG

KEY

```
$ ./keylog_dump.sh --pwn-all --
```

execute(

BRK

CORE

)

[OK] EXECUTED: 0xFEEDBA

execute(

CRK

INFO

)

[OK] EXECUTED: 0xDEAD00

execute(

BYP

DATA

)

[OK] EXECUTED: 0xB0BB1E

 Personal

 25

SQL INJECTION LOG

BINARY

```
$ ./exploit_db_sql_injector.s...
```

bypass(

BRK

MEM

)

[OK] BYPASSED // ADDR: 0xEFF...

execute(

CRK

AUTH

)

[OK] EXECUTED: 0xAUTH00

execute(

>_HKT

DATA

)

[OK] EXECUTED: 0xFACE00

execute(

BYP

INFO

)

[OK] EXECUTED: 0xFACADE

 Dark Web

 15

C2 ADDRESS LIST

NO LOG

```
$ ./c2_addresses.sh --bypass--
```

execute(

CRK

ACC

)

[FAIL] EXEC_FAILED // EXCEPT...

inject(

BRK

SYS

)

[FAIL] INJECT_BLOCKED // ID:...

 Dark Web

 15

SAM... REGISTRY HIVE

VAR

```
$ ./sam_hive_backup.sh --infi...
```

bypass(

CRK

MEM

)

[OK] BYPASSED // ADDR: 0xB01...

execute(

>_HKT

AUTH

)

[OK] EXECUTED: 0xC0DE42

execute(

BYP

INFO

)

[FAIL] EXEC_FAILED // EXCEPT...

decrypt(

BRK

LOCK

)

[OK] DECRYPTED // KEY: 0xBEE...

 Personal

 25

SAM... REGISTRY HIVE

SYS

```
$ ./registry_backup.sh --neur...
```

execute(

CRK

CORE

)

[OK] EXECUTED: 0xB0B000

execute(

>_HKT

AUTH

)

[OK] EXECUTED: 0xC0FFEE

execute(

BYP

INFO

)

[FAIL] EXEC_FAILED // EXCEPT...

 Government

 25

SHADOWSOCKS CONFIGURATION

VAR

```
$ ./ss_config.sh --neural-ove...
```

execute(

CRK

INFO

)

[FAIL] EXEC_FAILED // EXCEPT...

execute(

CRK

AUTH

)

[FAIL] EXEC_FAILED // EXCEPT...

inject(

>_HKT

SYS

)

[FAIL] INJECT_BLOCKED // ID:...

execute(

CRK

CONN

)

 Dark Web

 25

SAM... REGISTRY HIVE

COPY

```
$ ./extract_sam.sh --bypass-t...
```

execute(

>_HKT

INFO

)

[OK] EXECUTED: 0xDEADBE

execute(

CRK

AUTH

)

[OK] EXECUTED: 0xFACE42

inject(

BRK

SYS

)

[FAIL] INJECT_BLOCKED // ID:...

load(

BYP

KEY

)

[OK] LOADED // BUFFER: 0xFEE...

 Government

 25

LSASS.DMP MEMORY DUMP

PROTECTED

```
$ ./restore_sam.sh --buffer-o...
```

execute(

>_HKT

ACC

)

[OK] EXECUTED: 0xDECODE

load(

CRK

KEY

)

[OK] LOADED // BUFFER: 0xF00...

execute(

BYP

AUTH

)

[OK] EXECUTED: 0xB45E00

execute(

>_HKT

CORE

)

 Government

