TURLA «PENQUIN_X64» IS IN DA HOUSE

RISE OF APT TURLA — 2004

PENQUIN MALWARE AFFECTED LINUX OS — 2014

APT CASE RUAG BY CH GOVCERT — 2016

FEW MORE INFORMATION ABOUT PENQUIN BACKDOOR — 2017

ANOTHER VERSION OF PENQUIN, WAS DISCOVERED BY LEONARDO'S RESEARCHERS: "**PENQUIN_X64**" — 2020

VICTIMOLOGY: **DEFENCE, GOVERNMENT, RESEARCH, PHARMACEUTICAL CO.**

COUNTRIES: **> 45** | THREAT TYPE: STATE SPONSORED | SOPHISTICATION: INNOVATOR

ARCHITECTURE & **CAPABILITIES**

- CONF. PARAMETER: **HARDCODED**
- ROOT PRIVILEGE REQ.: **YES**
- ACTIVATION TYPE: **PASSIVE**
- EMBEDDED FILES: **YES** – CRON->/ROOT/.SESS
- COMMAND AND FUNCTION: **DOWNLOAD AND EXECUTE NEXT STAGE PAYLOAD**

READ THE FULL REPORT «MALWARE TECHNICAL INSIGHT TURLA PENQUIN_X64» TO IMPLEMENT APPROPRIATE CYBER DEFENCE POLICIES.

CYBERSECURITY DIVISION:
N. VERDE, A. VILLANI, S. LA PORTA
(CYBER THREAT ANALYSTS)

INFO-DESIGN (2020):
A. ROSSI (HEAD OF **LDO-CERT**)

TLP: WHITE

CYBER KILL CHAIN

THE BEHAVIOR OF THIS IMPLANT SUGGESTS THAT IT STARTS TO OPERATE AT THE "INSTALLATION" PHASE OF THE CYBER KILL CHAIN®, AND, SUCCESSIVELY, ONCE THE STEALTH BACKDOOR IS ACTIVATED BY THE ATTACKER, IT OPERATES AT THE "COMMAND AND CONTROL" PHASE ALSO. AT THE SAME TIME, IT DOES NOT EXCLUDE THAT THE "ACTIONS ON OBJECTIVES" PHASE COULD BE UP AND RUNNING ON THE COMPROMISED INFRASTRUCTURE OR ON OTHER INFRASTRUCTURES.

ATTACK PREPARATION AND PLANNING — ESTIMATED TIME: WEEKS

RECONNAISANCE — PLANNING

PREPARATION — WEAPONIZATION

VULNERABLE SYSTEM INTRUSIONS — ESTIMATED TIME: HOURS

DELIVERY — ATTEMPT

ATTEMPT / SUCCESS — EXPLOITATION

INSTALLATION — SUCCESS

COMPROMISE IN PROGRESS — ESTIMATED TIME: MONTHS

MANAGE & ENABLE — COMMAND & CONTROL (C2)

ACTION ON OBJECTIVES — EXECUTE

MITRE ATT&CK TTPs

TECHNIQUES

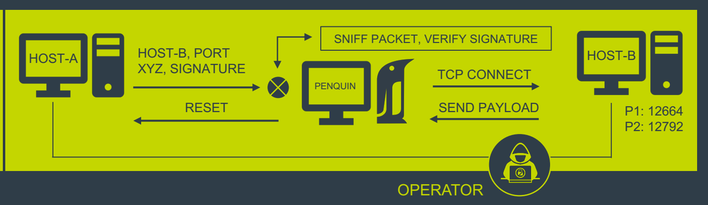
COMMAND-LINE INTERFACE	PORT KNOCKING	REMOTE FILE COPY	CUSTOM COMMAND AND CONTROL PROTOCOL	CUSTOM CRYPTOGRAPHIC PROTOCOL	STANDARD CRYPTOGRAPHIC PROTOCOL	HIDDEN FILES AND DIRECTORIES	FILE AND DIRECTORY PERMISSIONS MODIFICATION
T1059	T1205	T1105	T1094	T1024	T1032	T1158	T1222
8%	8%		25%		17%		42%

TACTICS

EXECUTION — LATERAL MOVEMENT — DEFENCE EVASION — PERSISTENCE — COMMAND AND CONTROL

MAGIC PACKET

DEMO



UDP

0	SPORT	DPORT
4	LENGHT	CHECKSUM
8	1° DWORD	
12	2° DWORD	

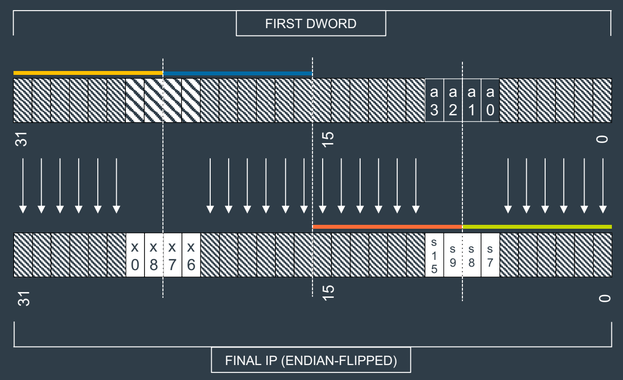
0	SPORT	DPORT
4	1° DWORD	
8	2° DWORD	
12	…	

TCP

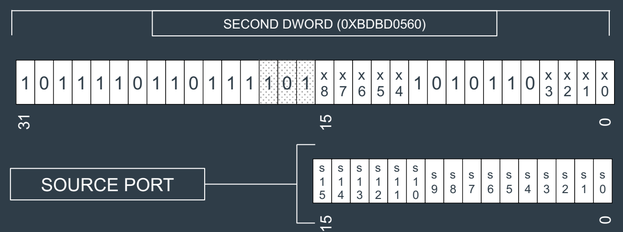
```
(tcp[8:4] & 0xe007ffff =
0x6005bdbd) or (udp[12:4] &
0xe007ffff = 0x6005bdbd)
```

FILTERING — SCRAMBLING — SWAPPING

EVERY FIELD IS REPRESENTED WITH A BIT-LEVEL GRANULARITY SINCE MOST OF THE OPERATIONS ARE PERFORMED BITWISE AND DO NOT ALIGN TO THE BYTE BOUNDARIES. ON TOP, THERE IS THE INPUT DATA (THAT CONSISTS OF TWO DWORDS AND THE SOURCE PORT) AND THE FINAL IP ADDRESS.



REPRESENTATION OF THE CHECKS MADE BY "PENQUIN" IN ORDER TO RETRIEVE THE COMMAND AND CONTROL IP ADDRESS FROM A SNIFFED INCOMING ACTIVATION PACKET.

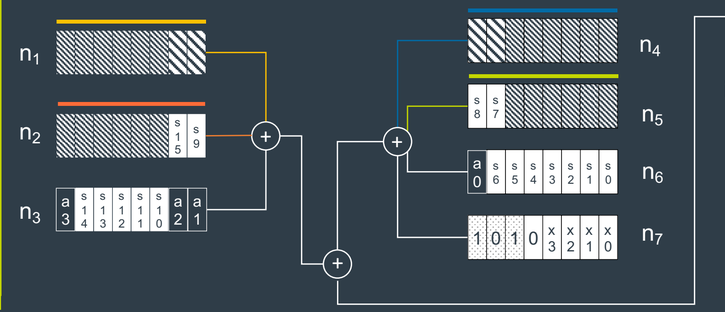


THE INPUT DATA (THAT CONSISTS OF TWO DWORDS AND THE SOURCE PORT) AND THE FINAL IP ADDRESS

DATA [01]

[02] CONDITIONS

RELATION BETWEEN THE INPUT PACKETS AND THE FINAL DESTINATION IP ADDRESS, AS WELL AS THE CONDITIONS REQUIRED BY PENQUIN, ARE SUMMARISED



if $((n_1 \oplus n_2 \oplus n_3) \oplus (n_4 \oplus n_5 \oplus n_6 \oplus n_7)) == n_8$
return success

LEONARDO