



AGID

Agenzia per l'Italia Digitale

Nuovi malware e vecchie insidie: affrontarli con l'aiuto della Threat Intelligence

Gianni Amato – AgID

Analisi delle minacce più diffuse in Italia



Osservatorio del CERT-AgID

Gianni Amato - AGID Agenzia per l'Italia Digitale

- CERT-AgID
- CERT-PA (precedentemente)
- Unità di missione sull'Intelligenza Artificiale istituita da AGID



Di cosa si occupa il CERT-AgID

- Incident Response
- Cyber Threat Intelligence
- Malware Analysis
- Infosharing



Qual è la Constituency

- Trust Services Providers
- Pubbliche Amministrazioni



I compiti del CERT-AgID per la PA



Piano Triennale 2024-2026

AGID metterà a disposizione della Pubblica Amministrazione una serie di piattaforme e di servizi, che verranno erogati tramite il proprio **CERT**, finalizzati alla conoscenza e al contrasto dei rischi cyber legati al patrimonio ICT della PA (obiettivo 7.6)

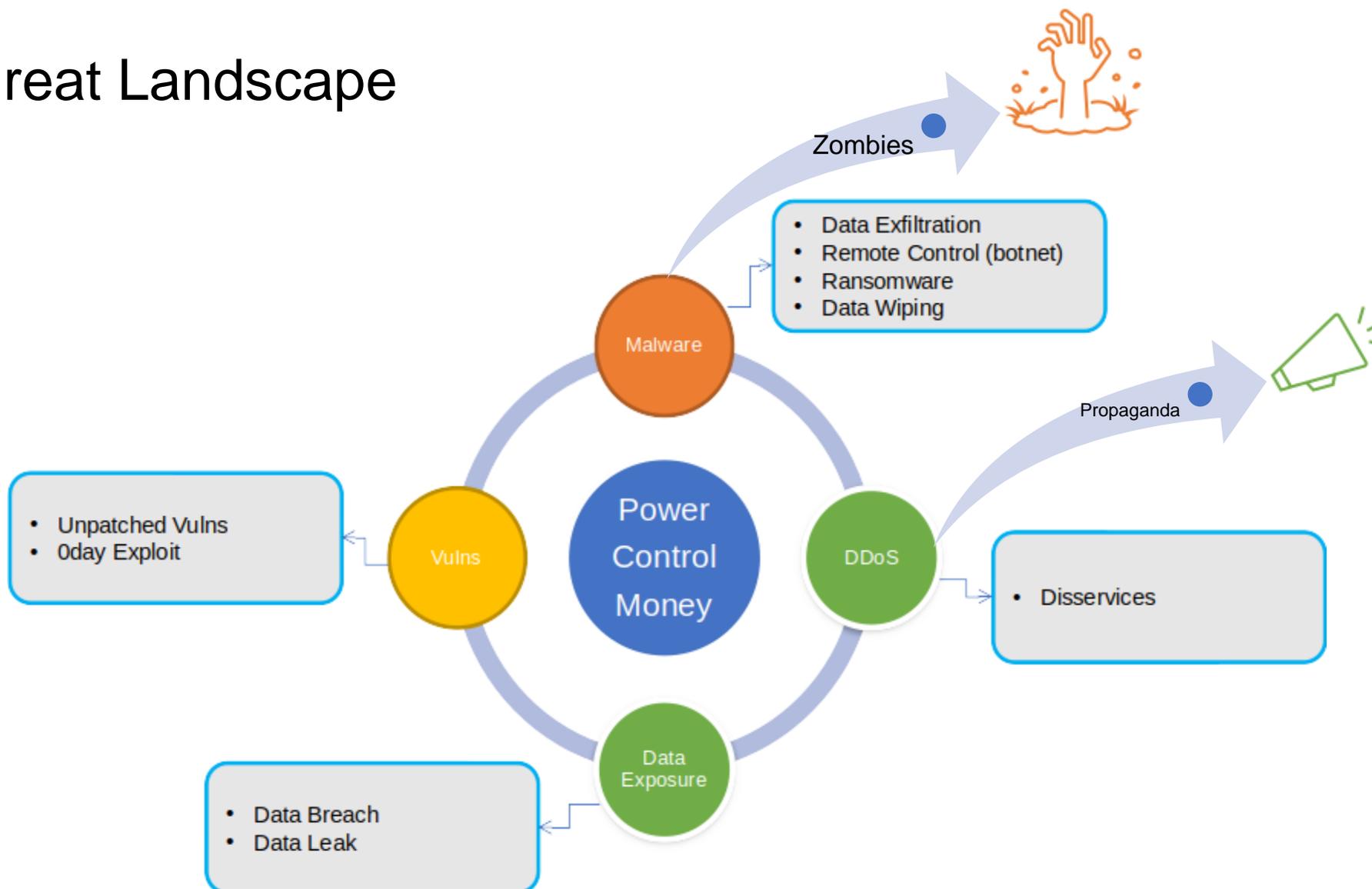
- Distribuzione di **Indicatori di Compromissione** alle PA;
- Fornitura di **strumenti** funzionali all'esecuzione dei piani di **autovalutazione dei sistemi esposti**;
- Supporto **formativo** e **informativo** rivolto alle PA e in particolare agli **RTD** per l'aumento del livello di consapevolezza delle minacce cyber.
- Intelligenza Artificiale nella PA (capitolo 5)



5. **Privacy e sicurezza.** Le pubbliche amministrazioni adottano elevati standard di sicurezza e protezione della *privacy* per garantire che i dati dei cittadini siano gestiti in modo sicuro e responsabile. In particolare, le amministrazioni garantiscono la conformità dei propri sistemi di IA con la normativa vigente in materia di protezione dei dati personali e di sicurezza cibernetica.

Cyber Threat Landscape

In breve...



Attacco al Sistema Pubblico Identità Digitale (SPID)



Killnet 15/06/2022 | Propaganda

WE ARE KILLNET

Autenticazione

SPID CNS

SPID è il sistema di accesso che consente di utilizzare, con un'identità digitale unica, i servizi online della Pubblica Amministrazione e dei privati accreditati. Se sei già in possesso di un'identità digitale, accedi con le credenziali del tuo gestore. Se non hai ancora un'identità digitale, richiedi ad uno dei gestori.

Entra con SPID

Maggiori informazioni su SPID
Non hai SPID?

spid AgID Agenzia per l'Italia Digitale

Ещё одна хорошая новость.
Система управления полномочиями главного Банка Италии - заблокирована..

"SPID — это система доступа, которая позволяет вам использовать онлайн-услуги государственного управления и аккредитованных частных лиц с уникальным цифровым идентификатором."

👍 1678 🙌 219 ❤️ 62 🔥 57 😊 38 🤪 8 😄 7

👁️ 25.9K edited 17:46

A FM ET 73 comments

WE ARE KILLNET

spid
BANCA D'ITALIA

Nome utente Nome utente (obbligatorio)

Password Password (obbligatorio)

Mostra password

Tentativi rimanenti: 5

Entra

[Non hai SPID? Registrati!](#) [Incontra!](#)

Следом за ним "Система аутентификации"

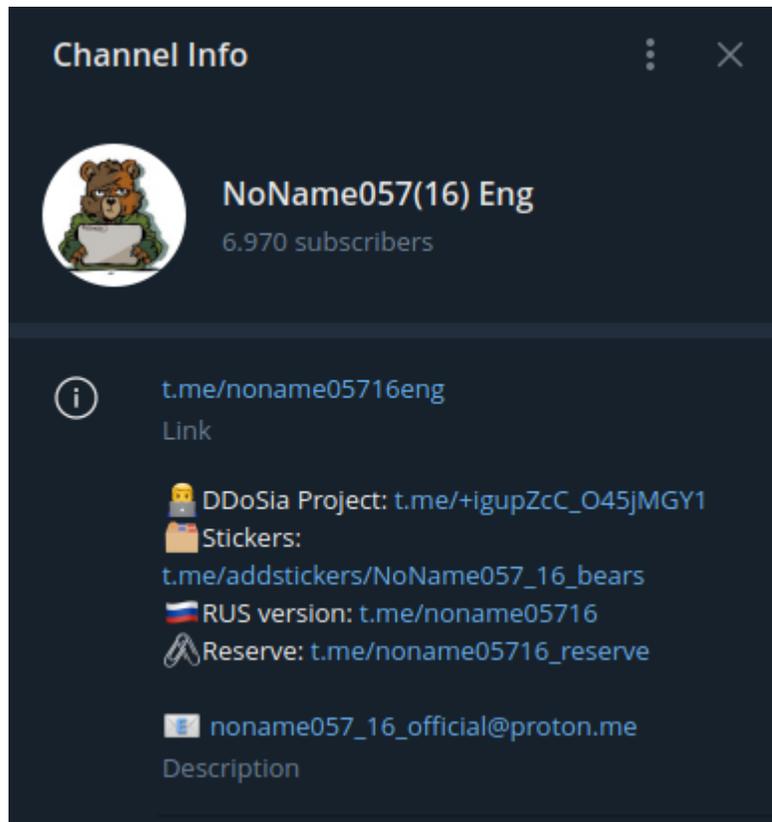
🔥 1397 🙌 239 🍌 59 ❤️ 41 😊 21 🎉 14

👁️ 25.3K edited 18:02

57 comments

È possibile prevedere un attacco DDoS?

Qualche volta si... il caso **NoName057**



The screenshot shows the Telegram channel page for 'NoName057(16) Eng'. The channel has 6,970 subscribers. The profile picture is a cartoon bear. Below the channel name, there are several links and descriptions:

- Link: t.me/noname05716eng
- DDoSia Project: t.me/+igupZcC_O45jMGY1
- Stickers: t.me/addstickers/NoName057_16_bears
- RUS version: t.me/noname05716
- Reserve: t.me/noname05716_reserve
- Description: noname057_16_official@proton.me

```
{
  "id": "639ad5136b6a908a8efb1691", "ratio": "1", "type": "tcp", "method": "syn", "host": "siac.difesa.it", "address": "185.86.84.17", "port": "443", "use_ssl": true, "path": "", "body": "",
  "type": "", "value": "", "use_random_user_agent": true, "timeout": 1000, "response": true, "headers": [], "is_deleted": false, "activate_by_schedule": false, "started_at": "", "finished_at": ""},
  "id": "639ad5136b6a908a8efb1692", "ratio": "1", "type": "tcp", "method": "syn", "host": "siac.difesa.it", "address": "185.86.84.17", "port": "80", "use_ssl": true, "path": "", "body": "",
  "type": "", "value": "", "use_random_user_agent": true, "timeout": 1000, "response": true, "headers": [], "is_deleted": false, "activate_by_schedule": false, "started_at": "", "finished_at": ""},
  "id": "639ad54b6b6a908a8efb1693", "ratio": "1", "type": "http", "method": "GET", "host": "e-learning.esercito.difesa.it", "address": "130.192.137.42", "port": "443", "use_ssl": true, "path": "/cou",
  "type": "", "value": "", "use_random_user_agent": true, "timeout": 1000, "response": true, "headers": [], "is_deleted": false, "activate_by_schedule": false, "started_at": "", "finished_at": ""},
  "id": "639ad54b6b6a908a8efb1694", "ratio": "1", "type": "tcp", "method": "syn", "host": "e-learning.esercito.difesa.it", "address": "130.192.137.42", "port": "443", "use_ssl": true, "path": "", "body": "",
  "type": "", "value": "", "use_random_user_agent": true, "timeout": 1000, "response": true, "headers": [], "is_deleted": false, "activate_by_schedule": false, "started_at": "", "finished_at": ""},
  "id": "639ad54b6b6a908a8efb1695", "ratio": "1", "type": "tcp", "method": "syn", "host": "e-learning.esercito.difesa.it", "address": "130.192.137.42", "port": "80", "use_ssl": true, "path": "", "body": "",
  "type": "", "value": "", "use_random_user_agent": true, "timeout": 1000, "response": true, "headers": [], "is_deleted": false, "activate_by_schedule": false, "started_at": "", "finished_at": ""},
  "id": "639ad54b6b6a908a8efb1696", "ratio": "1", "type": "http", "method": "GET", "host": "e-learning.esercito.difesa.it", "address": "130.192.137.42", "port": "443", "use_ssl": true, "path": "/", "body": "",
  "type": "", "value": "", "use_random_user_agent": true, "timeout": 1000, "response": true, "headers": [], "is_deleted": false, "activate_by_schedule": false, "started_at": "", "finished_at": ""},
  "id": "639ad54b6b6a908a8efb1697", "ratio": "1", "type": "nginx_loris", "method": "", "host": "e-learning.esercito.difesa.it", "address": "130.192.137.42", "port": "443", "use_ssl": true, "path": "", "body": "",
  "type": "", "value": "", "use_random_user_agent": true, "timeout": 1000, "response": true, "headers": [], "is_deleted": false, "activate_by_schedule": false, "started_at": "", "finished_at": ""},
  "id": "639ad6026b6a908a8efb169d", "ratio": "1", "type": "tcp", "method": "syn", "host": "web.aeronautica.difesa.it", "address": "78.6.226.139", "port": "443", "use_ssl": true, "path": "", "body": "",
  "type": "", "value": "", "use_random_user_agent": true, "timeout": 1000, "response": true, "headers": [], "is_deleted": false, "activate_by_schedule": false, "started_at": "", "finished_at": ""},
  "id": "639ad6026b6a908a8efb169e", "ratio": "1", "type": "tcp", "method": "syn", "host": "web.aeronautica.difesa.it", "address": "78.6.226.139", "port": "80", "use_ssl": true, "path": "", "body": "",
  "type": "", "value": "", "use_random_user_agent": true, "timeout": 1000, "response": true, "headers": [], "is_deleted": false, "activate_by_schedule": false, "started_at": "", "finished_at": ""},
  "id": "639ad6026b6a908a8efb169f", "ratio": "1", "type": "nginx_loris", "method": "", "host": "web.aeronautica.difesa.it", "address": "78.6.226.139", "port": "443", "use_ssl": true, "path": "", "body": "",
  "type": "", "value": "", "use_random_user_agent": true, "timeout": 1000, "response": true, "headers": [], "is_deleted": false, "activate_by_schedule": false, "started_at": "", "finished_at": ""}
}
```

Target list: `/client/get_targets`

```
"host": "www.spid.gov.it", "path": "/",
"host": "www.spid.gov.it", "path": "/xmlrpc.php",
"host": "www.spid.gov.it", "path": "/ricerca/?doctype%5B%5D=all\u0026search=$_1",
"host": "www.spid.gov.it", "path": "/wp-content/themes/dist/assets/json/faq_it_db.json",
```

La campagne malevole nel 2023



Le campagne malevole italiane nel 2023

AGID Agenzia per l'Italia Digitale

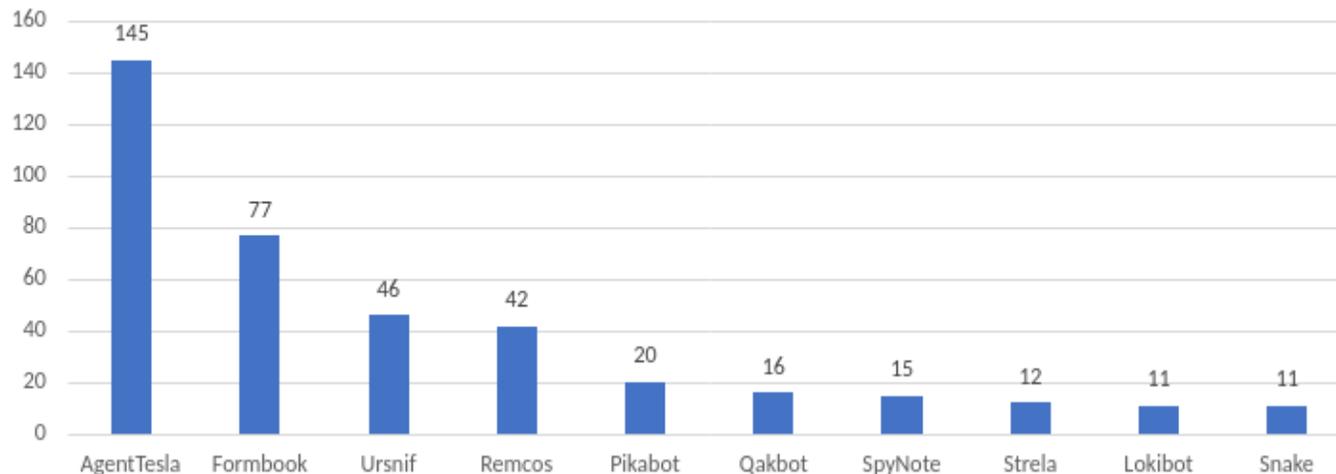
CERT-AGID
Computer Emergency Response Team
AGID

54
FAMIGLIE DI MALWARE

10
TEMI PIÙ USATI PER VEICOLARLI

- pagamenti
- ordine
- banking
- preventivi
- Agenzia Entrate

Top 10 malware nel 2023



	Malware	Phishing
Famiglie rilevate / Brand coinvolti	54	68
Campagne censite	510	1203
Indicatori (IoC) diramati	17827	2776

AgentTesla si è affermato come il malware più diffuso in Italia nel 2023. Tra i primi dieci, troviamo anche **SpyNote**, noto spyware progettato per dispositivi **Android**.

Dati esfiltrati da AgentTesla



Attività malevola in Italia

URL: <http://www.governo.it>
Username:
Password:
Application:Firefox

Agent Tesla 3.2.9.0 English

MAIN LOGGER PASSWORD RECOVERY **SETTINGS** OTHERS BUILD EXPLOIT SCANNER

INSTALLATION

FILE BINDER

ASSEMBLY ICON

Add to Startup Hide File Persistence Melt File UAC Bypass Delay exec.: 0 sec.

Startup Folder: ApplicationData Add UAC Manifest Kill Process: calc.exe

OPTIONS

Block Anti-viruses Protected Process Block Rightclick Restart PC USB Spread

— Process Killer: —

Task Manager CMD Registry System Restore

— Disable: —

Task Manager CMD Registry System Restore MSConfig

Run Folder Options Control Panel

Analisi delle tendenze generali



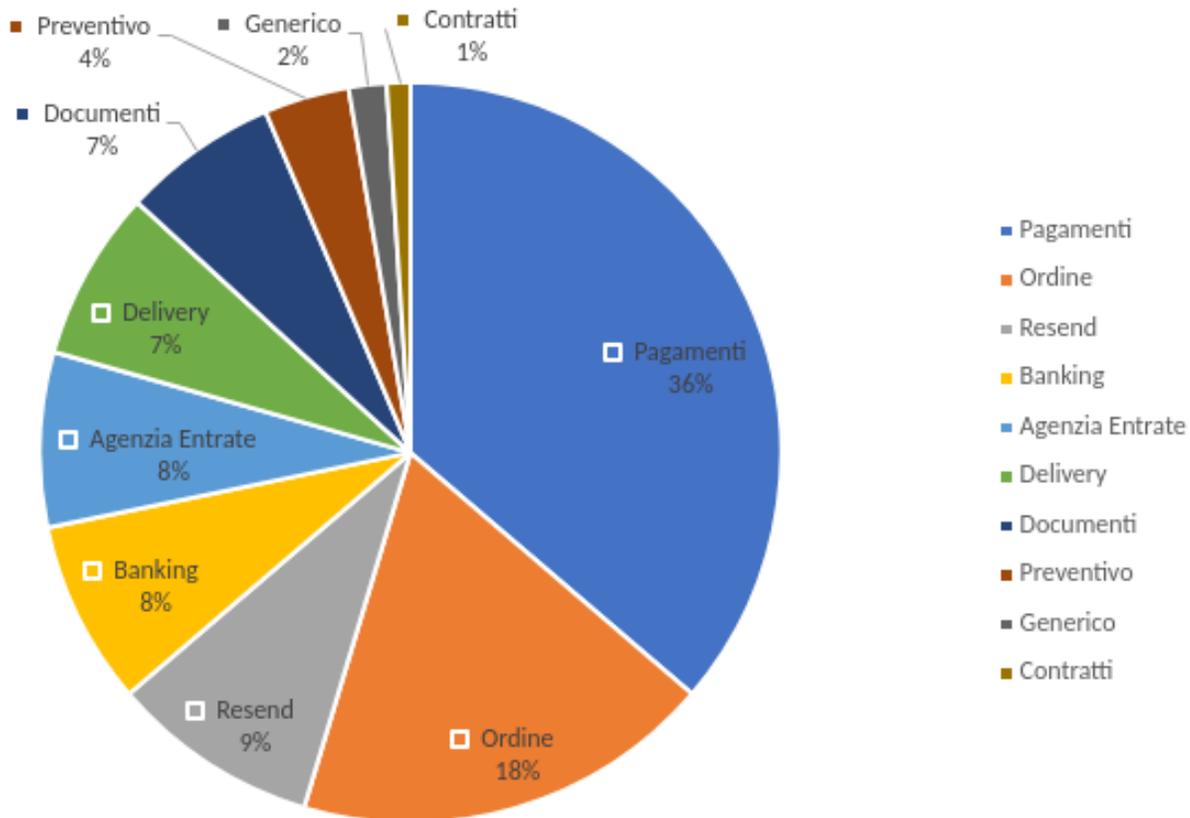
5 punti fondamentali

1. Nonostante il **ransomware** rimanga la minaccia **più rilevante** e ampiamente discussa anche nel 2023, si è riscontrato **un singolo caso** in Italia di ransomware (*Knight*) distribuito attraverso un loader veicolato tramite email. Le compromissioni da ransomware continuano ad essere realizzate manualmente, sfruttando accessi ai sistemi ottenuti mediante l'utilizzo di malware di tipo Infostealer o RAT.
2. A fianco della costante diffusione degli Infostealer è stata osservata una crescita dell'uso illecito di **strumenti di controllo remoto** come *ScreenConnect* o *UltraVNC*, strumenti che presentano funzionalità molto simili al noto *TeamViewer*. Questi strumenti consentono di assumere il controllo delle macchine delle vittime, visualizzandone il contenuto del loro schermo ed interagendo con esso come farebbe un utente locale utilizzando mouse e tastiera.
3. E' in forte crescita in Italia il trend di attacchi **spyware con funzionalità di RAT**, veicolati tramite campagne di smishing e finalizzati ad ottenere il controllo completo dei dispositivi **Android**.
4. Si è registrata una **costante diminuzione** del numero di campagne malware condotte attraverso account compromessi di Posta Elettronica Certificata (**PEC**).
5. Nel corso del 2023, **Telegram** ha consolidato la sua posizione di ecosistema predominante utilizzato dalle attività di cybercrime, come evidenziato dalla grande diffusione sui suoi canali della vendita e divulgazione di dati personali e aziendali rubati. Inoltre, ha assunto un ruolo predominante anche come luogo privilegiato per la rivendicazione di attacchi informatici e di compromissione, soprattutto da parte di collettivi filorussi e gang ransomware.

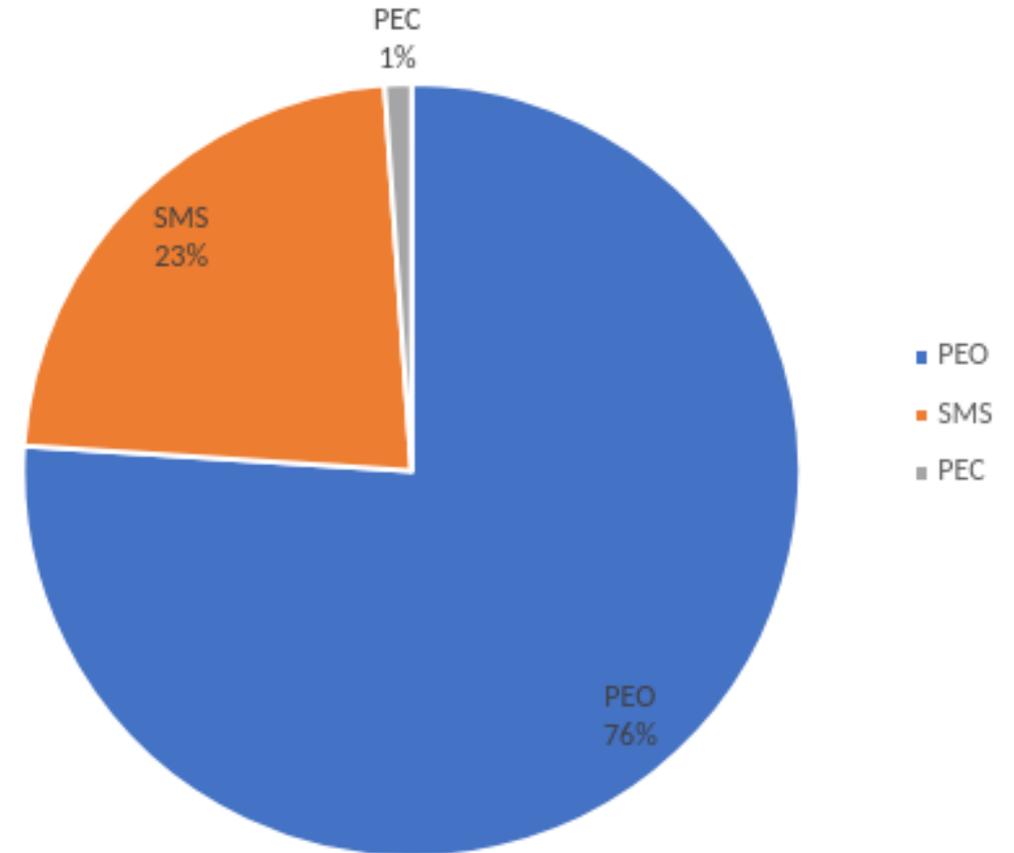
I principali Temi e canali di diffusione malware in Italia

Lo smishing in crescita

Top 10 temi nel 2023

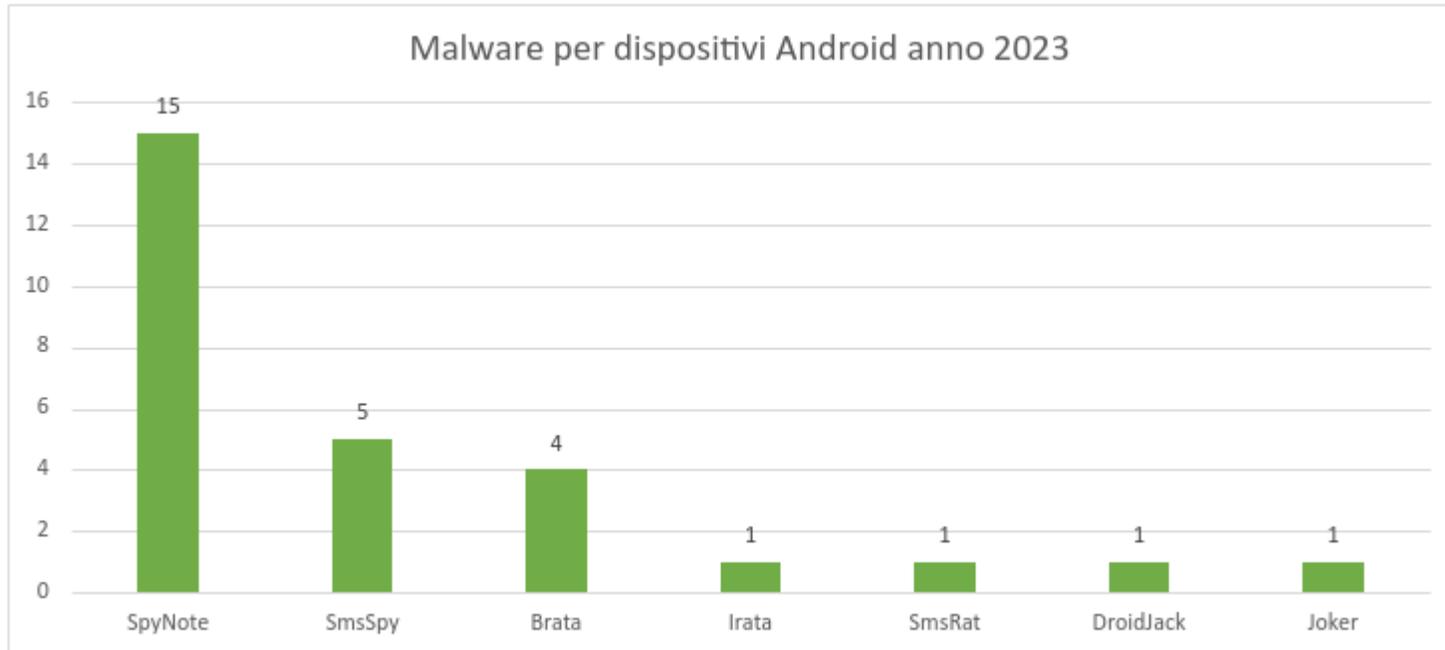


Canali di diffusione campagne malevole nel 2023



Malware per dispositivi mobili basati su sistemi Android

SpyNote

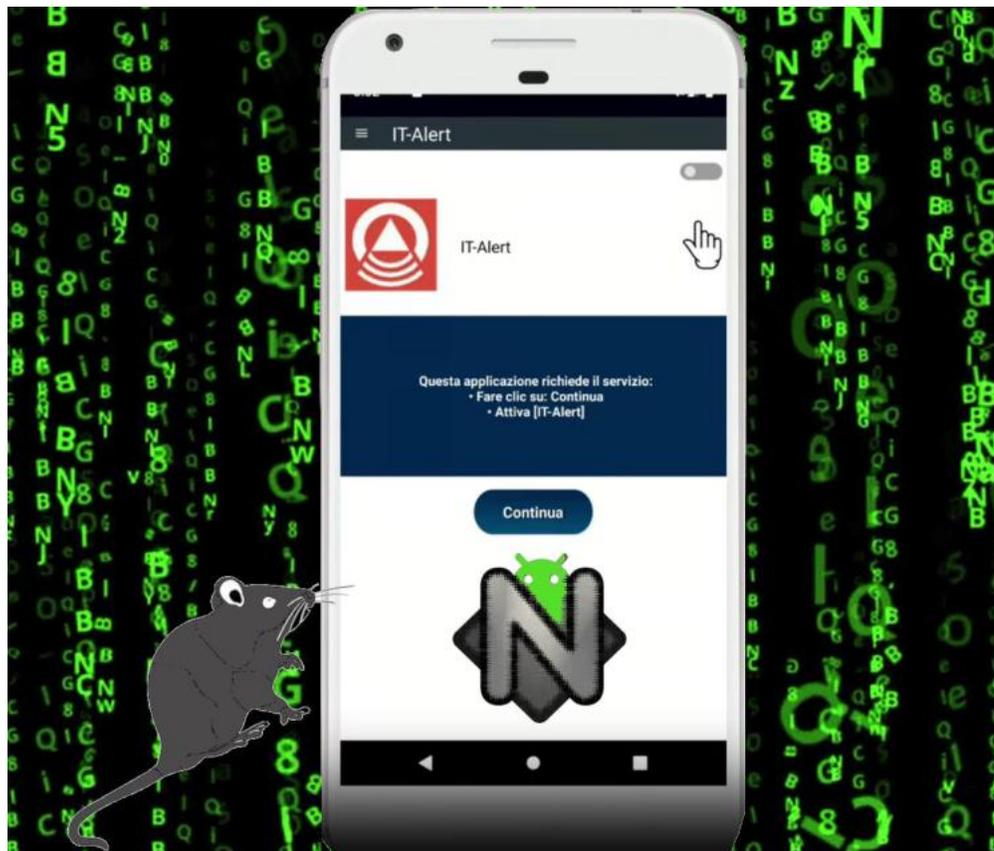


La funzionalità predominante di queste applicazioni malevole è la **lettura degli SMS**, finalizzata a intercettare i codici inviati dalla banca come secondo fattore di autenticazione (**2FA**).

Nel corso del 2023, sono state individuate **29 campagne malevole** mirate a compromettere dispositivi mobili basati su sistemi Android. Tra i vari malware identificati, **SpyNote** emerge come il più diffuso, con la registrazione di tre varianti nel corso dell'anno.

SpyNote - Analisi delle funzionalità

Infostealer



Funzionalità standard

- Intercettare **SMS** (2FA)
- Rubare **passwd** e **CC**
- **Registrazione** chiamate
- **Catturare** schermate

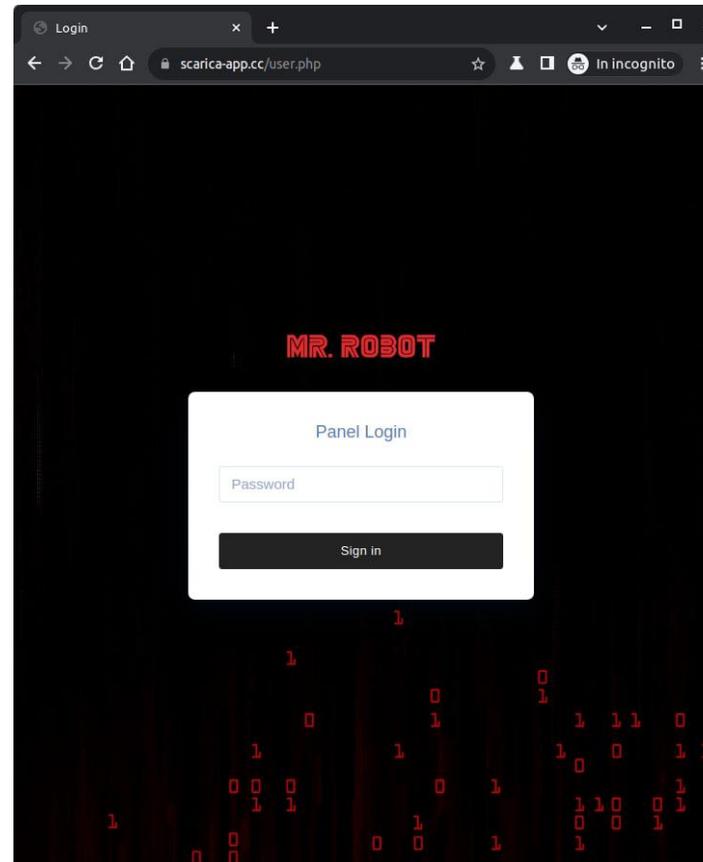
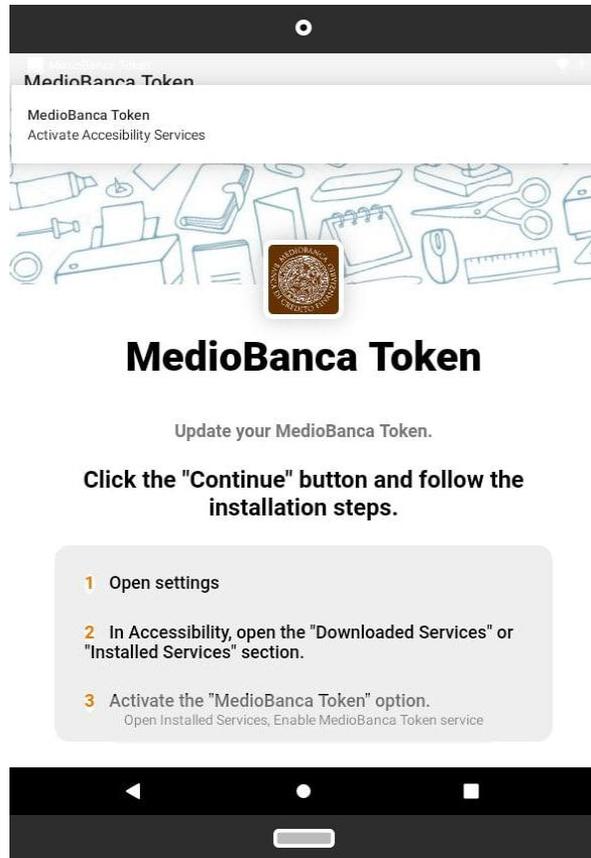
Funzionalità degne di attenzione

- Autorizzazioni automatiche
- Rilevamento degli emulatori
- Esclusione dalle app recenti
- Localizzazione del dispositivo
- Keylogging
- Comunicazioni con il C2

Grazie alla **modularità** delle funzioni fornite attraverso il builder e al suo continuo sviluppo **SpyNote** è uno dei malware per Android che si distingue per l'elevata **capacità di raccogliere informazioni** e per la flessibilità che offre agli attori malevoli di **estendere le funzionalità** tramite le costanti interazioni con il C2

IRATA - Iranian Remote Access Tool Android

Infostealer



IRATA ha recentemente rivolto le sue campagne malevole verso l'Italia tramite l'utilizzo di messaggi SMS ingannevoli.

- Le vittime ricevono un **SMS** che sembra provenire da una banca italiana.
- Il messaggio invita a seguire un **link** per scaricare una applicazione Android malevola.

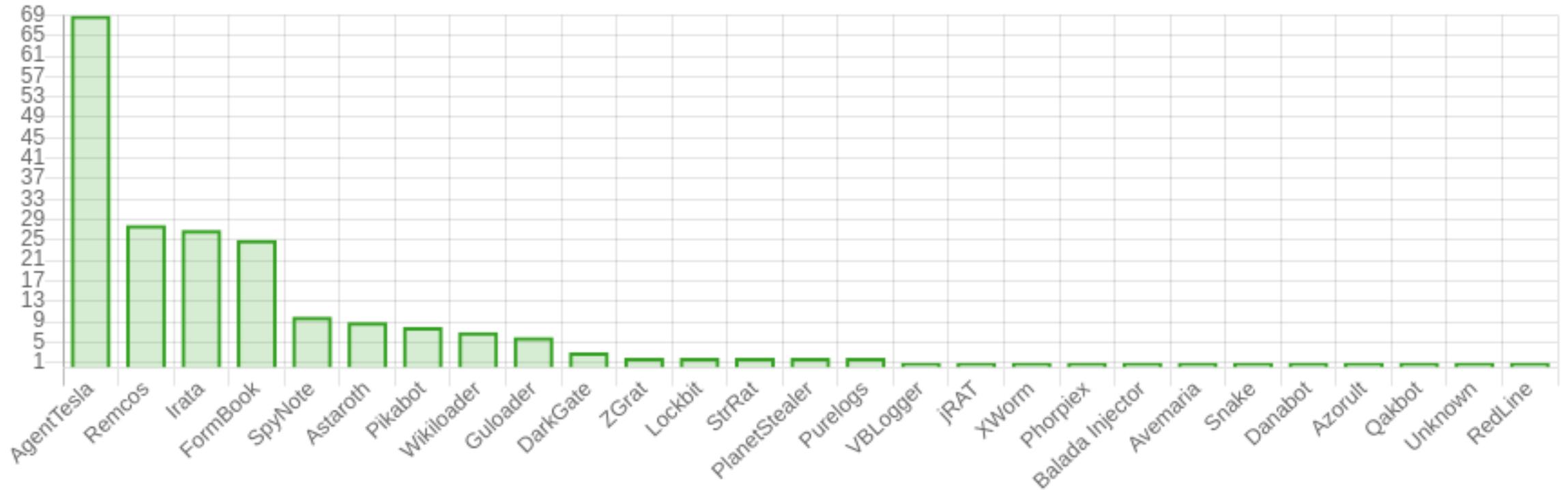
Qual è lo scopo?

- Furto estremi delle **carte di credito**
- Dispositivo **bot** per inviare SMS
- Ottenere **accesso agli SMS** di autenticazione a due fattori (**2FA**)

Malware – maggio 2024

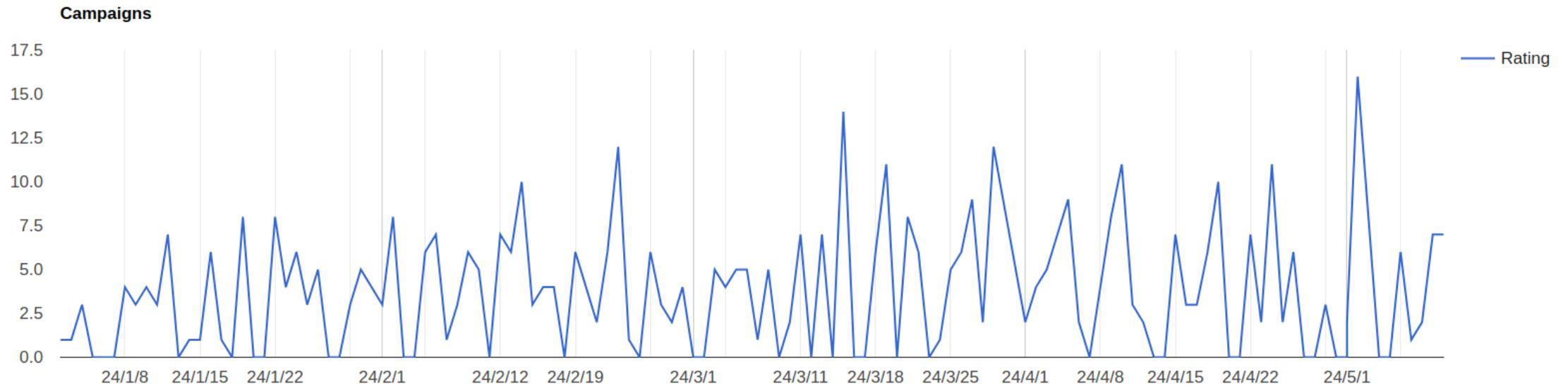
Famiglie di malware

27 malware family



Malware – maggio 2024

Campagne malevole



Compravendita di credenziali di accesso



Initial Access Broker

545k ITALY COMBO MAIL:PASS - with private MAILS ACCESS VALID

mongame100 Offline
Posted 15 October 2021 - 05:28 PM

MrRoBoTmall, on 07 Jun 2020 - 10:54 PM, said:

Combolist Type : Email & Pass
Date of the leak : 08/06/2020
Rows of the combolist:545k Emails & Pass
Has been used on websites before the leak: Yes/No : No

Rep **SELLING** Fresh Stealer Logs in October For Sale
by djzigoh - October 17, 2021 at 01:23 AM

djzigoh New User
October 17, 2021 at 01:23 AM

MEMBER

Posts 68
Threads 6
Joined Feb 2021
Reputation 37

Total: 20.000+ Redline Stealer Logs in October
All Logs uploaded Mega.nz.
Price: 80\$ for Sale
Contact telegram: @djzigoh

Note: only sold by month, not sold according to individual requirem
Payment: BTC, ETH, USDT...

NoHide.Space
2.989 subscribers

Pinned message
❤️ PRIVATE TELEGRAM CLOUD WITH MAIL ACCESS - [sqli.cloud] ❤️ 🚫 Mail access,

330 11:42

NoHide.Space

Get started

upload a base clipboard Make a screenshot Telegram, register and start

Start **Start** Finish folder Check email in the database

Settings

Hide my user name

Save private keys to the DB

Save public keys

Save private keys in general folder

Save public keys

Information

Loaded from 739k Good int

8,368,803,000 Keys in the DB

My key

Need a help

739K	22K	3218	322	20K	94.6%	428
Loaded	Checked	Pages	Resolves	Others	Percent of	Checked

@Datacloud
Selling 739k Full Valid Mail Access
Valid: 97%
Poland, Italy, Germany, France, Czech
Private is: 94%
Price: \$110
Only for one Person!
@Datacloud

334 12:06

Proposte al mercato nero



Annunci autopromozionali

Scrivo codice in C, C++, php, node.js, posso usare i framework.

Scrivo quasi tutto e dipende dal tuo budget:

"Malware

Пишу кода на с, с++, php, node.js

" Stealer

Пишу практически все и зависю от бюджета

"Loader

» Malware

" Ransomware

» Stealer

"E altri software

» Loader

» Ransomware

Contatti Jabber:

» И другой софт

* Principale: hellxss@thesecure.biz (otr)

Джаббер контакты:

* Riserva: tox

* Основная: hellxss@thesecure.biz

* Telegram: non uso

* Резерв: tox

Senza OTR , non scrivermi nemmeno...

* Telegram: не использую

Verificare immediatamente tramite il PM.

I can develop "Ransomware" undetected data encryption software from scratch especially for you.

- 1- Programming from scratch
- 2- light in size
- 3- fast encoder
- 4- Not detected by any security software
- 5- Custom extension of your choice
- 6- An icon specifically for that extension "Files encrypted with one icon become"
- 7- You can request other program features if possible

c, c++, node.js, php.

The M3rcury ransomware is a ransomware written entirely from scratch, which

Feature List

Removal of backups

Hybrid RSA AES-256 encryption

UAC bypass

Sandbox Detection

Evasion of heuristic analysis

Heavy obfuscation

Scantime packed and crypted

Encryption mechanism to defeat anti-ransomware detection

Working on windows 7/8/10

Encryption mechanism:

M3rcury goes through all files on the system and encrypts only part of them, because it will have encrypted many more files before detected as opposed to the header.

What you will receive

Attacker side decryption source code written in golang

Copy of the main ransomware executable in both 32 and 64 bit

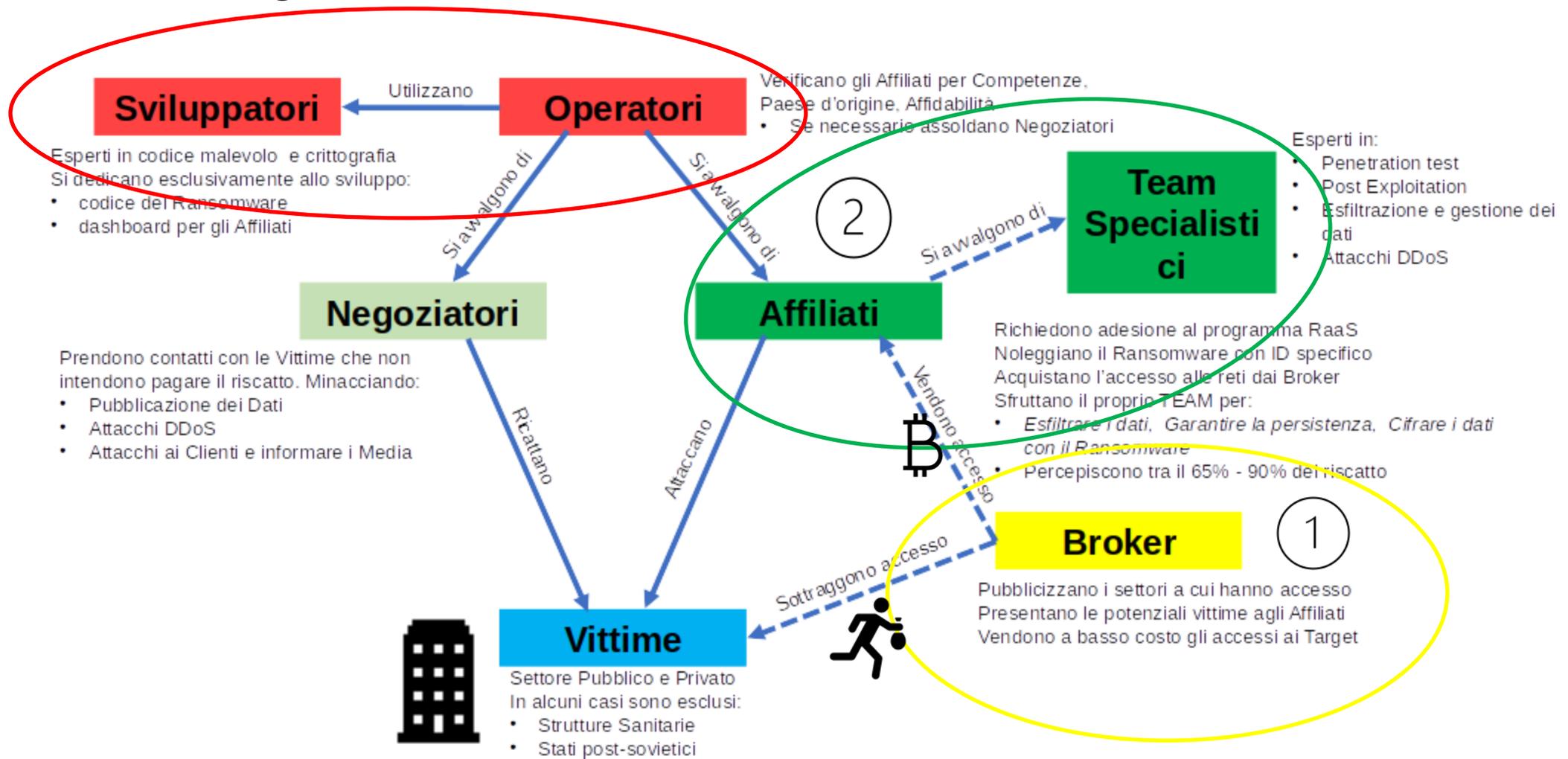
Your unique private key for victim decryption

Access to all future updates!

Note: This is not RaaS you receive 100% of your ransoms! :)

Payload size is 2.7 MB

Galassia e organizzazione del Ransomware as a Service



Grazie per l'attenzione