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

CERT-AGID

AGID

Qual è la Constituency

- Trust Services Providers
- Pubbliche Amministrazioni

I compiti del CERT-AgID per la PA

Piano Triennale 2024-2026

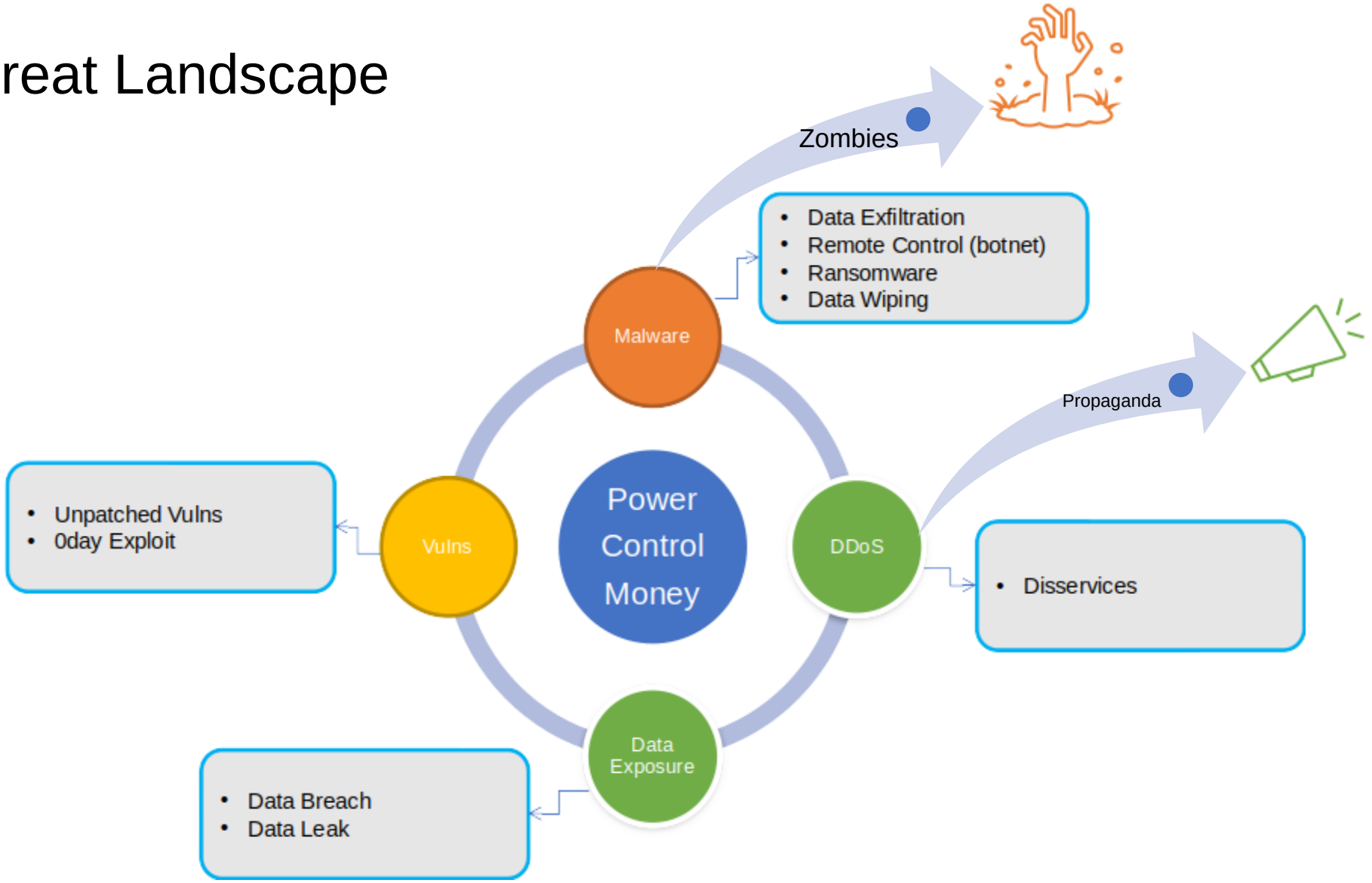
AGID metterà a disposizione della Pubblica Amministrazione una serie di piattaforme e di servizi, che verranno erogati tramite il proprio **CERT**, finalizzati alla conoscenza e al contrasto dei rischi cyber legati al patrimonio ICT della PA (obiettivo 7.6)

- 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.

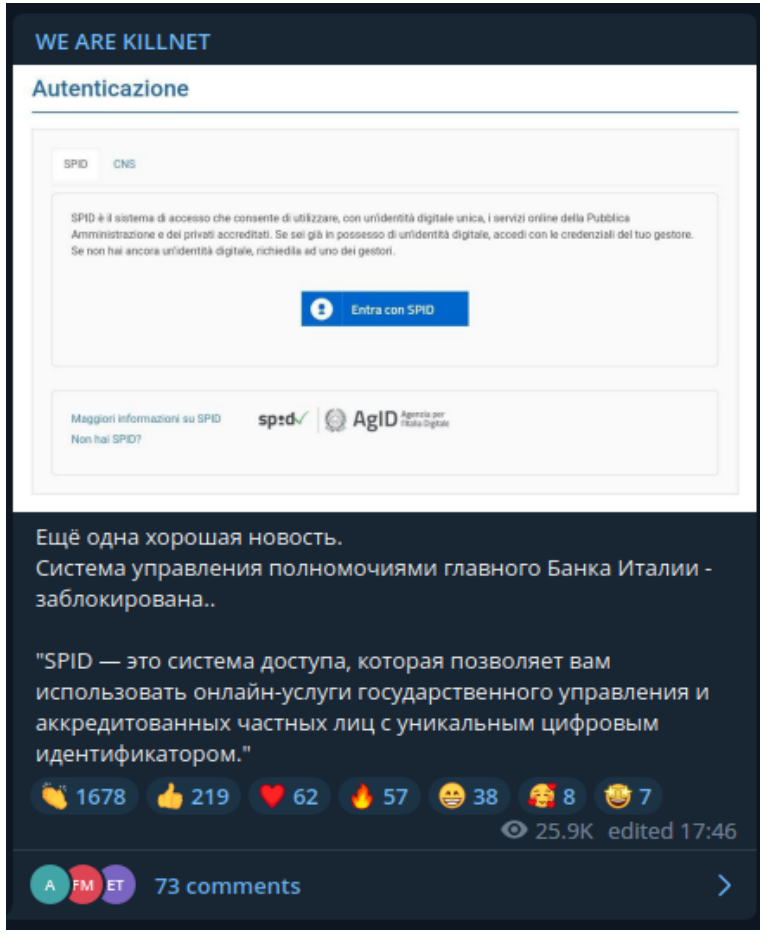
Cyber Threat Landscape

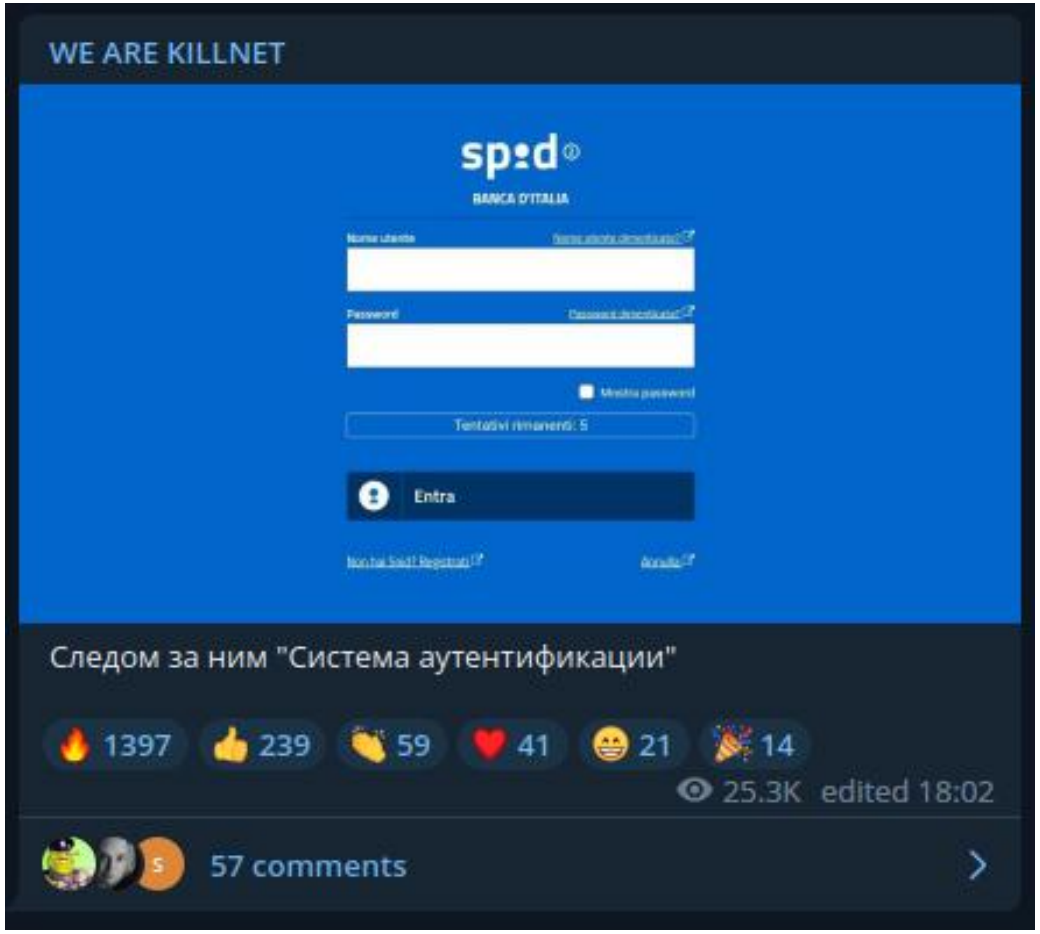
In breve...



Attacco al Sistema Pubblico Identità Digitale (SPID)

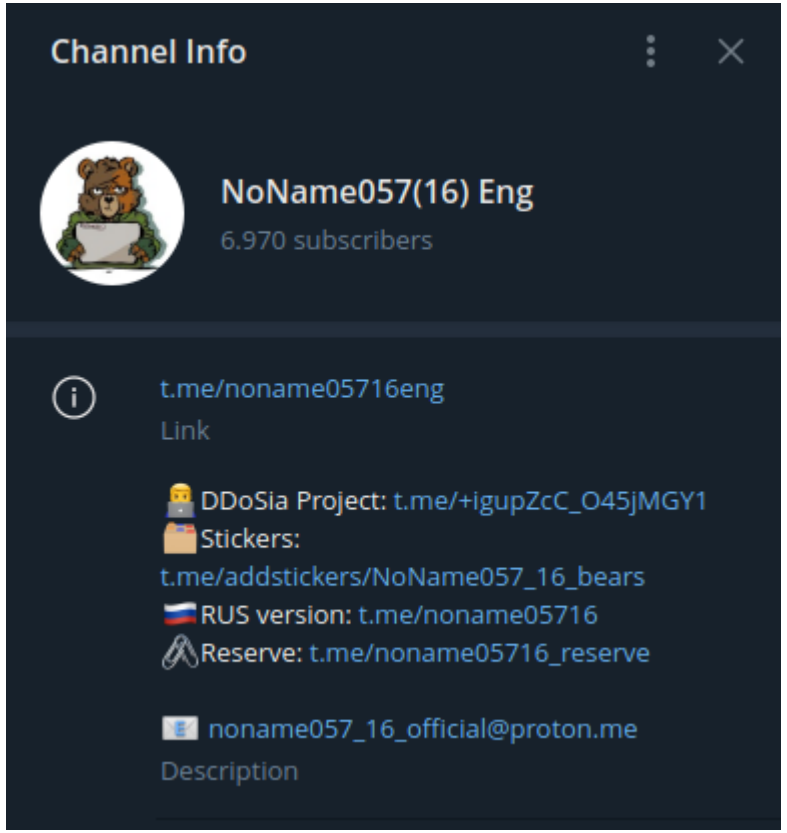
Killnet 15/06/2022 | Propaganda





È possibile prevedere un attacco DDoS?

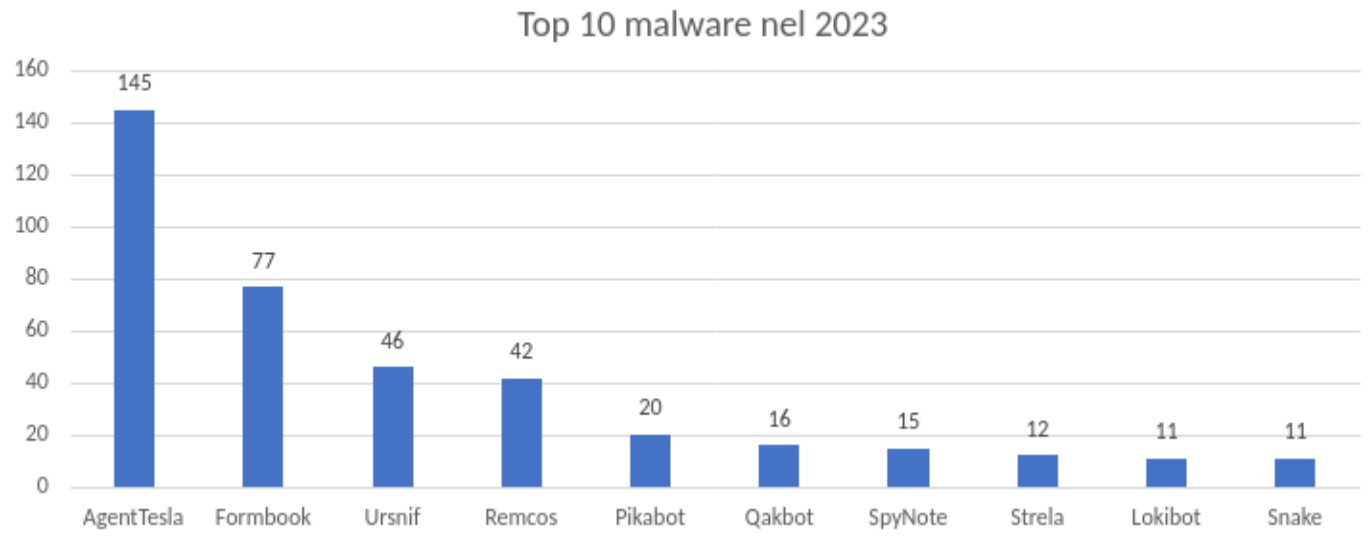
Qualche volta si... il caso **NoName057**



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



	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: .gov.it
Username:
Password:
Application:Firefox

URL: .gov.it
Username
Password:
Application:Firefox

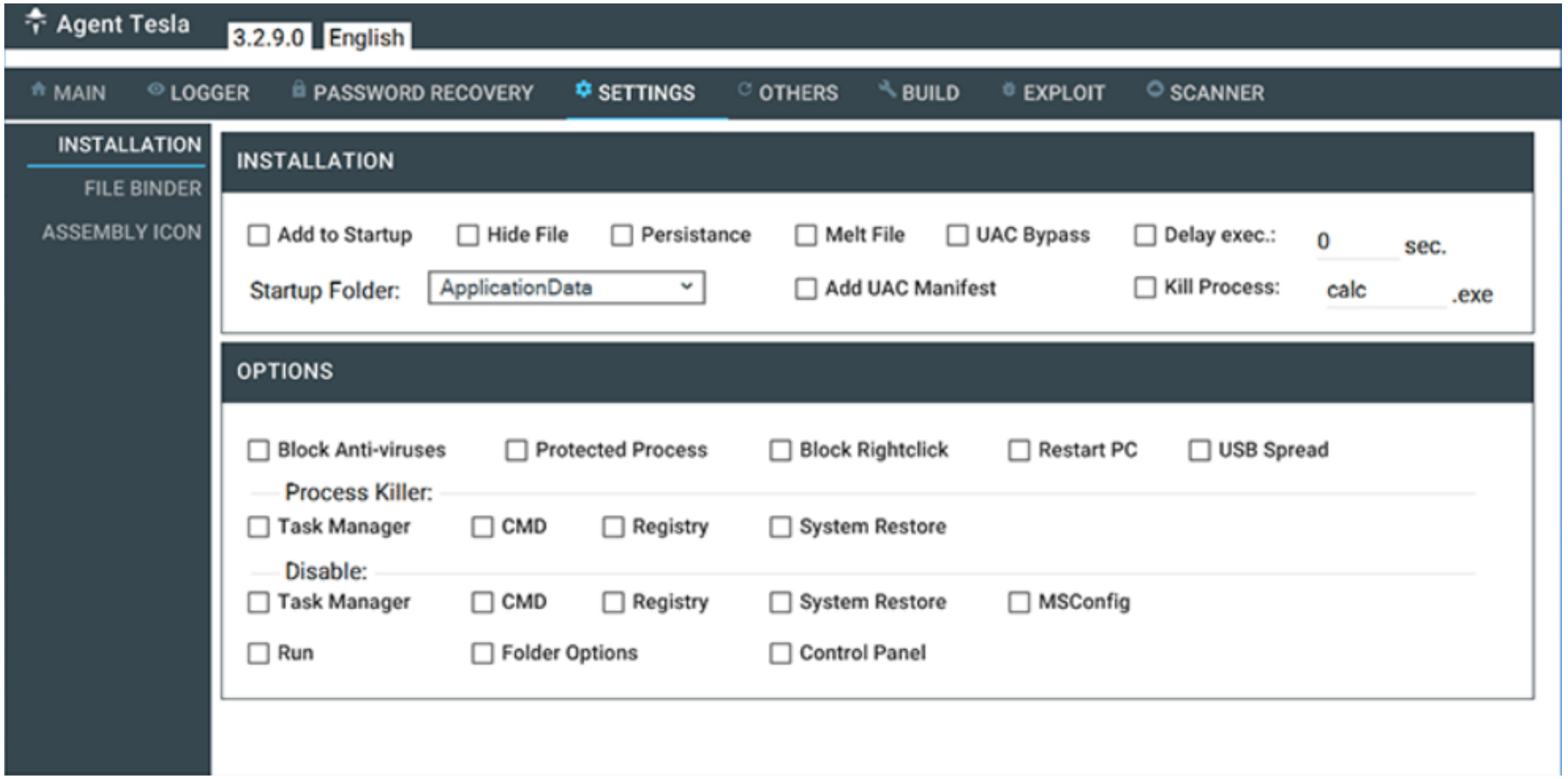
URL: .it
Username:
Password:
Application:Firefox

URL .istruzione.it
Username:
Password:
Application:Firefox

URL: .istruzione.it
Username:
Password:
Application:Firefox

URL: .istruzione.it
Username:
Password:
Application:Firefox

URL: .istruzione.it
Username:
Password:



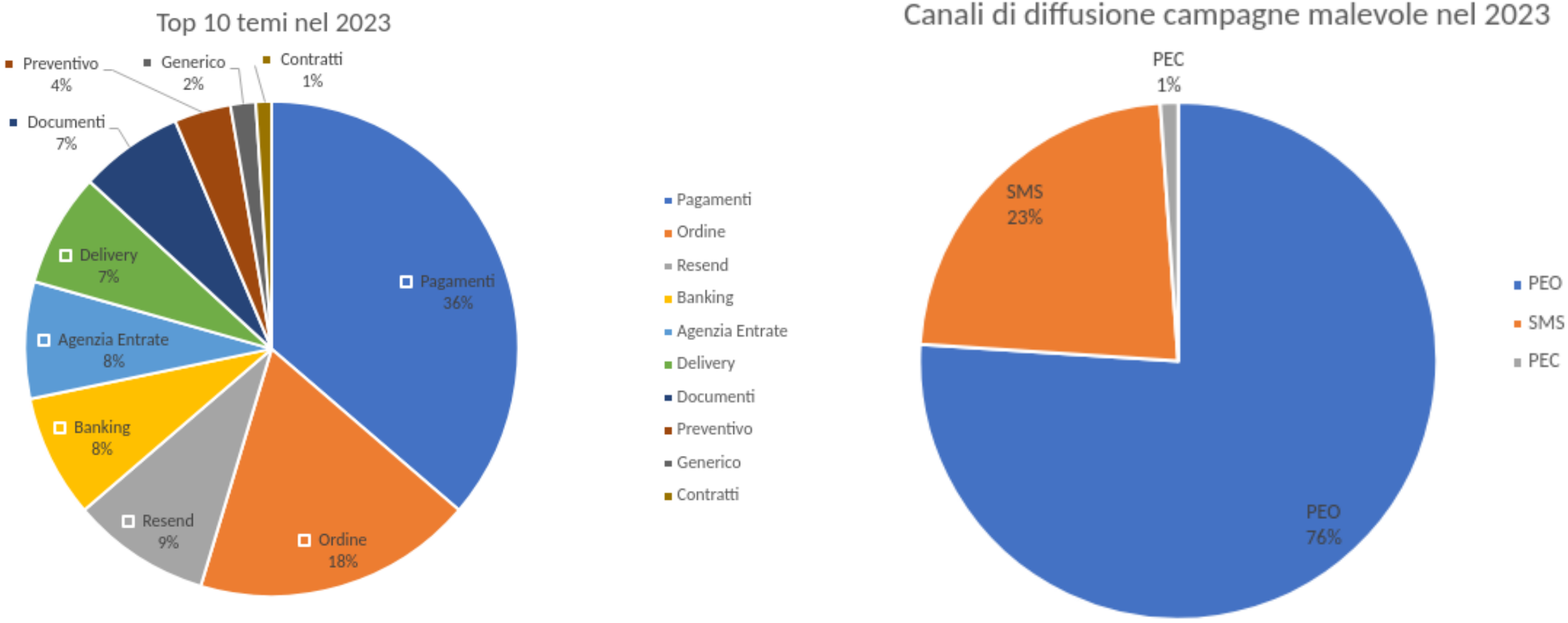
Analisi delle tendenze generali

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.

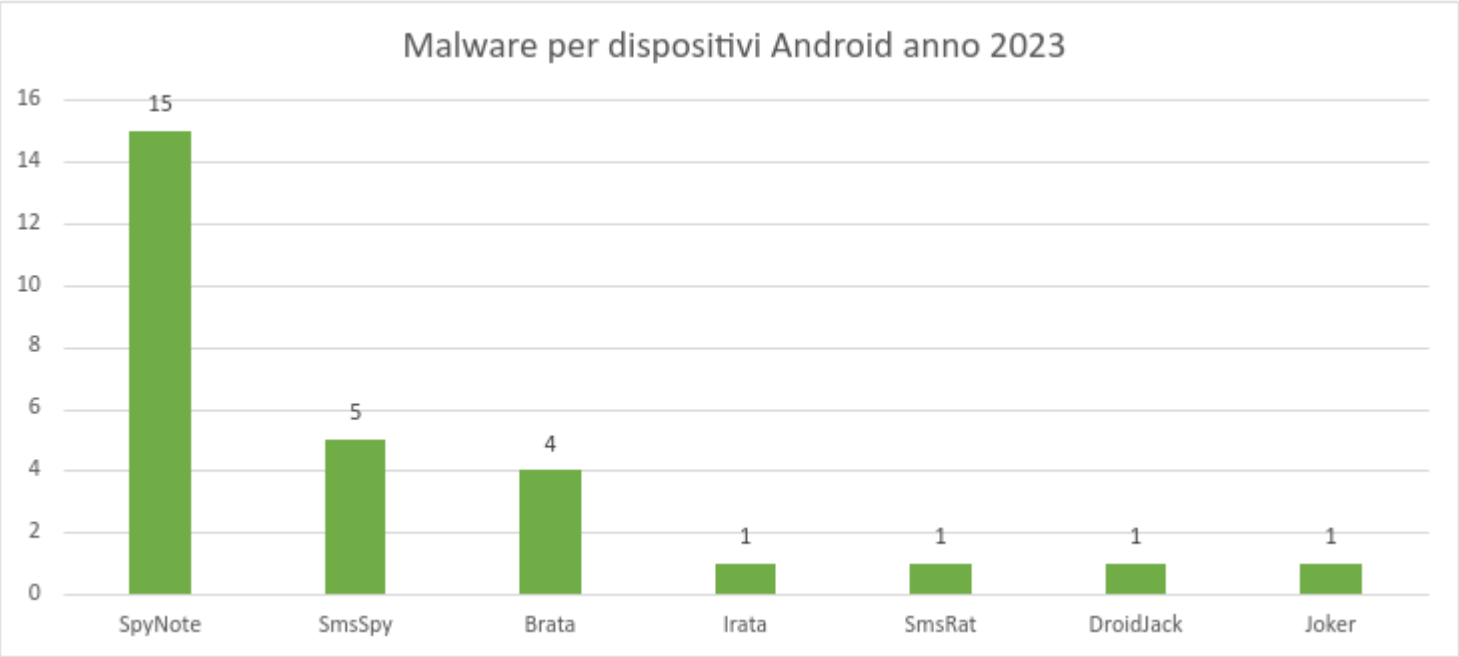
I principali Temi e canali di diffusione malware in Italia

Lo smishing in crescita



Malware per dispositivi mobili basati su sistemi Android

SpyNote

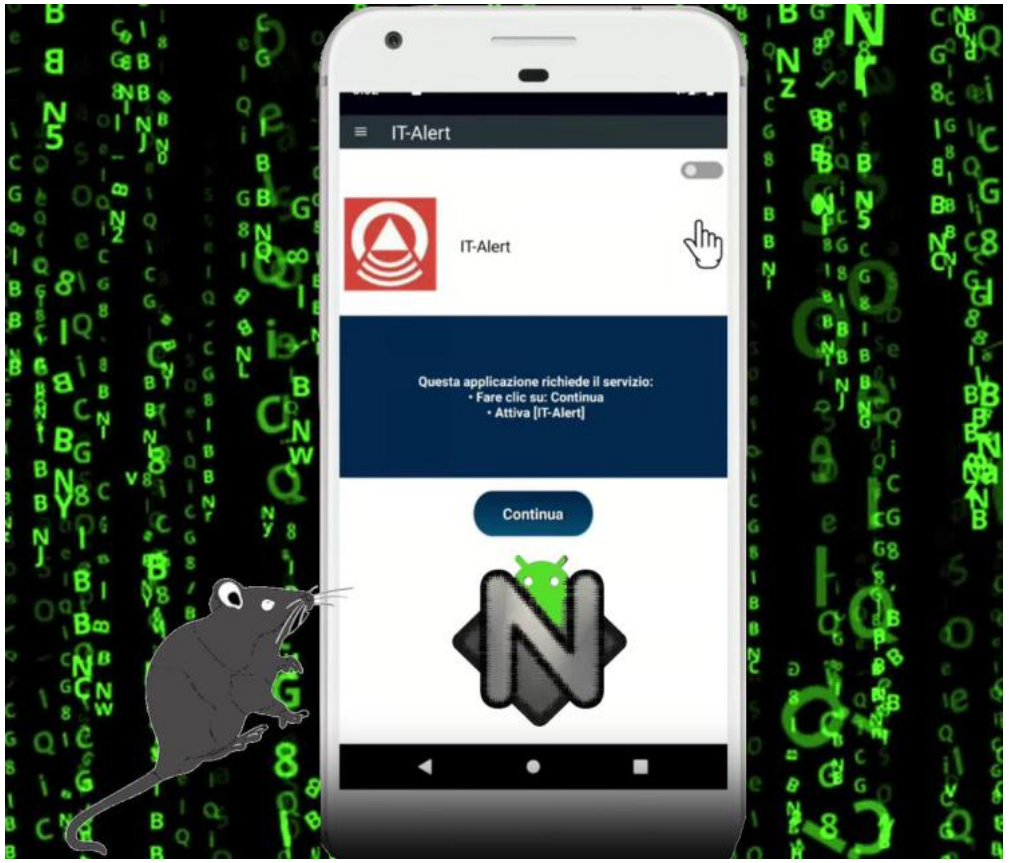


La funzionalità predominante di queste applicazioni malevole è la **lettura degli SMS**, finalizzata a intercettare i codici inviati dalla banca come secondo fattore di autenticazione (**2FA**).

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

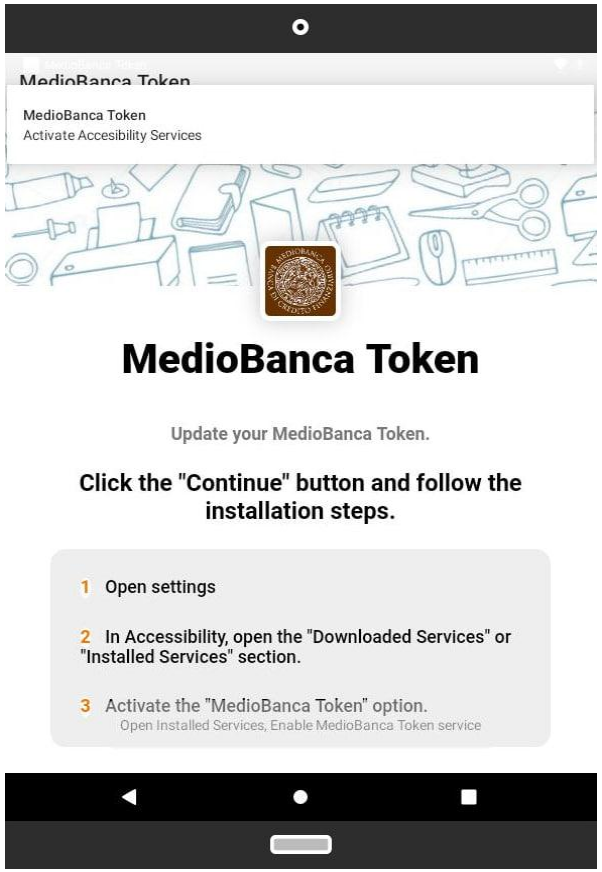
Funzionalità degne di attenzione

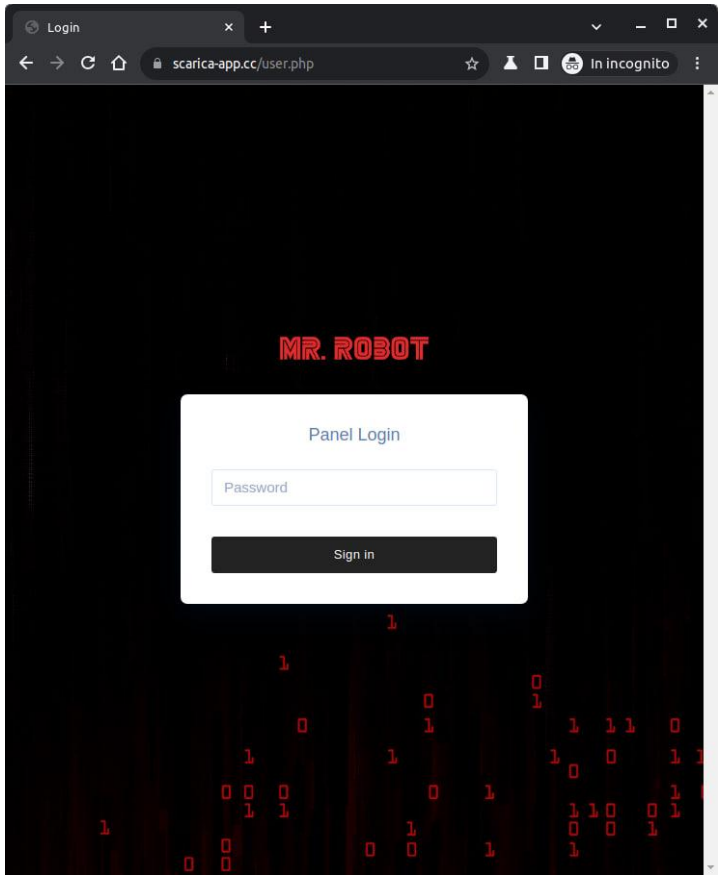
- Autorizzazioni automatiche
- Rilevamento degli emulatori
- Esclusione dalle app recenti
- Localizzazione del dispositivo
- Keylogging
- Comunicazioni con il C2

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.

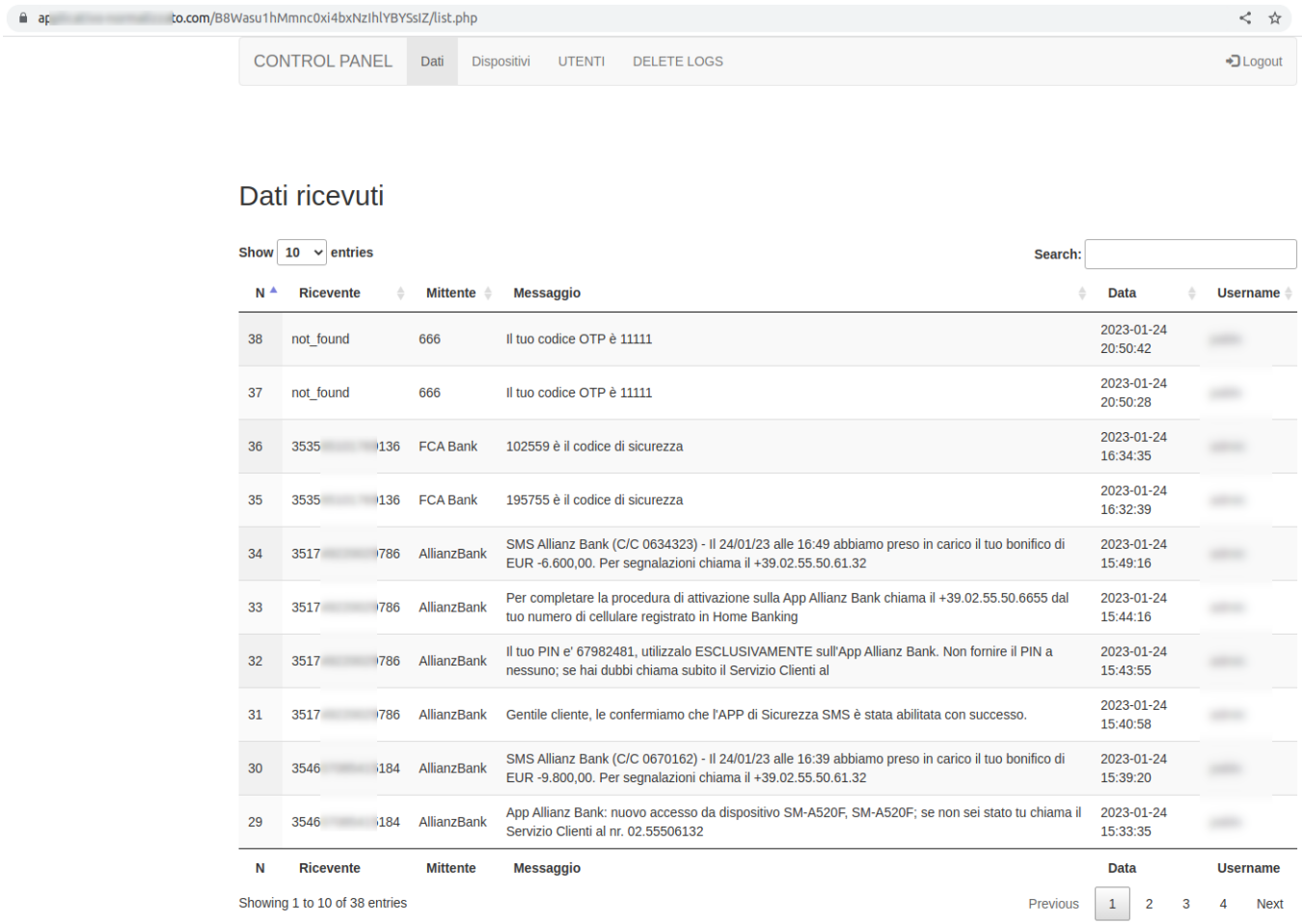
- Le vittime ricevono un **SMS** che sembra provenire da una banca italiana.
- Il messaggio invita a seguire un **link** per scaricare una applicazione Android malevola.

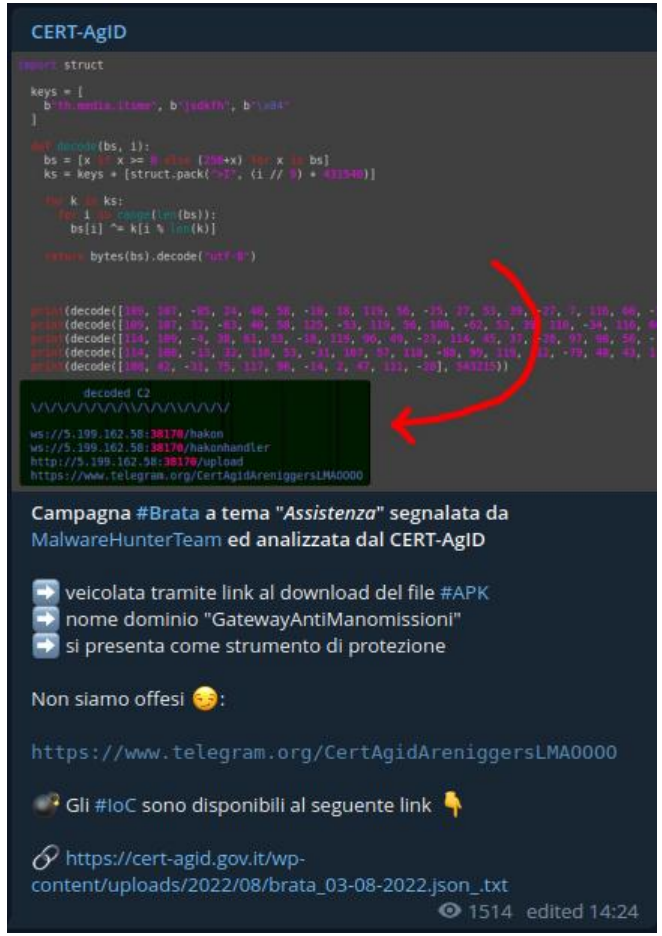
Qual è lo scopo?

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

C2 - 2FA

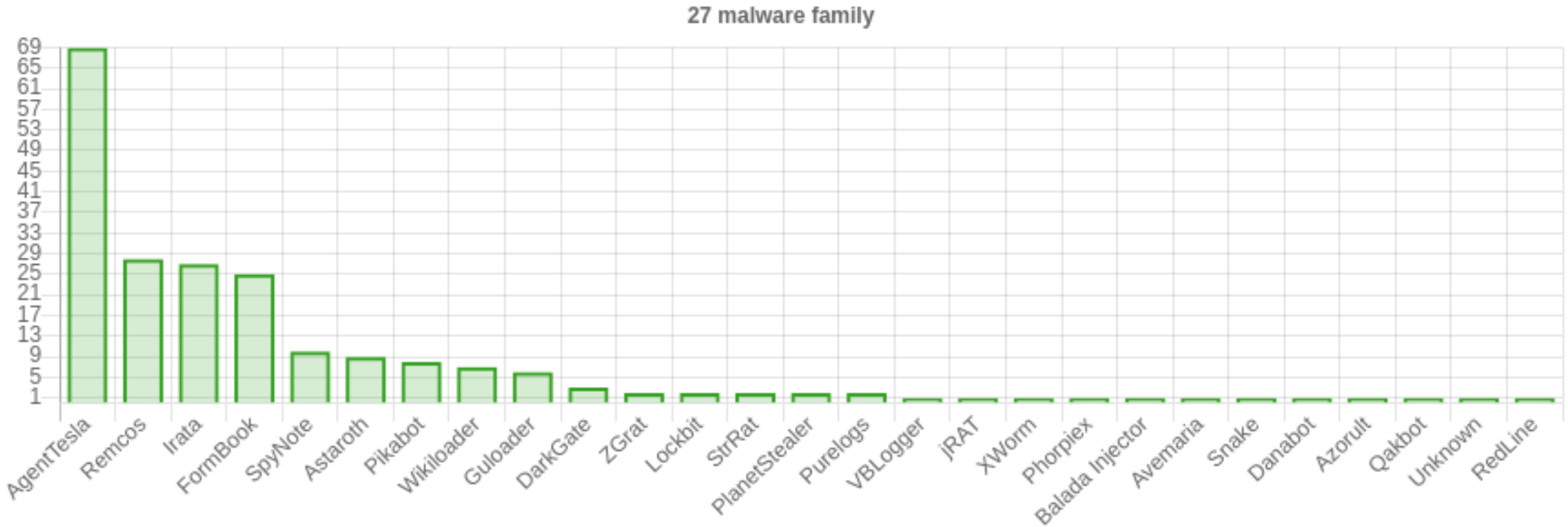
Command & Control





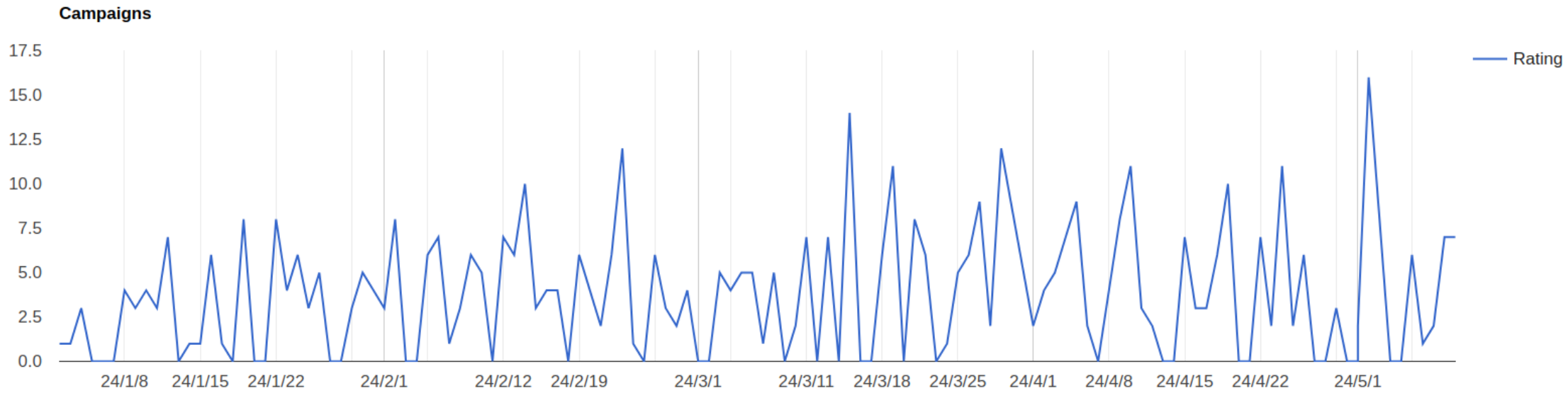
Malware – maggio 2024

Famiglie di malware



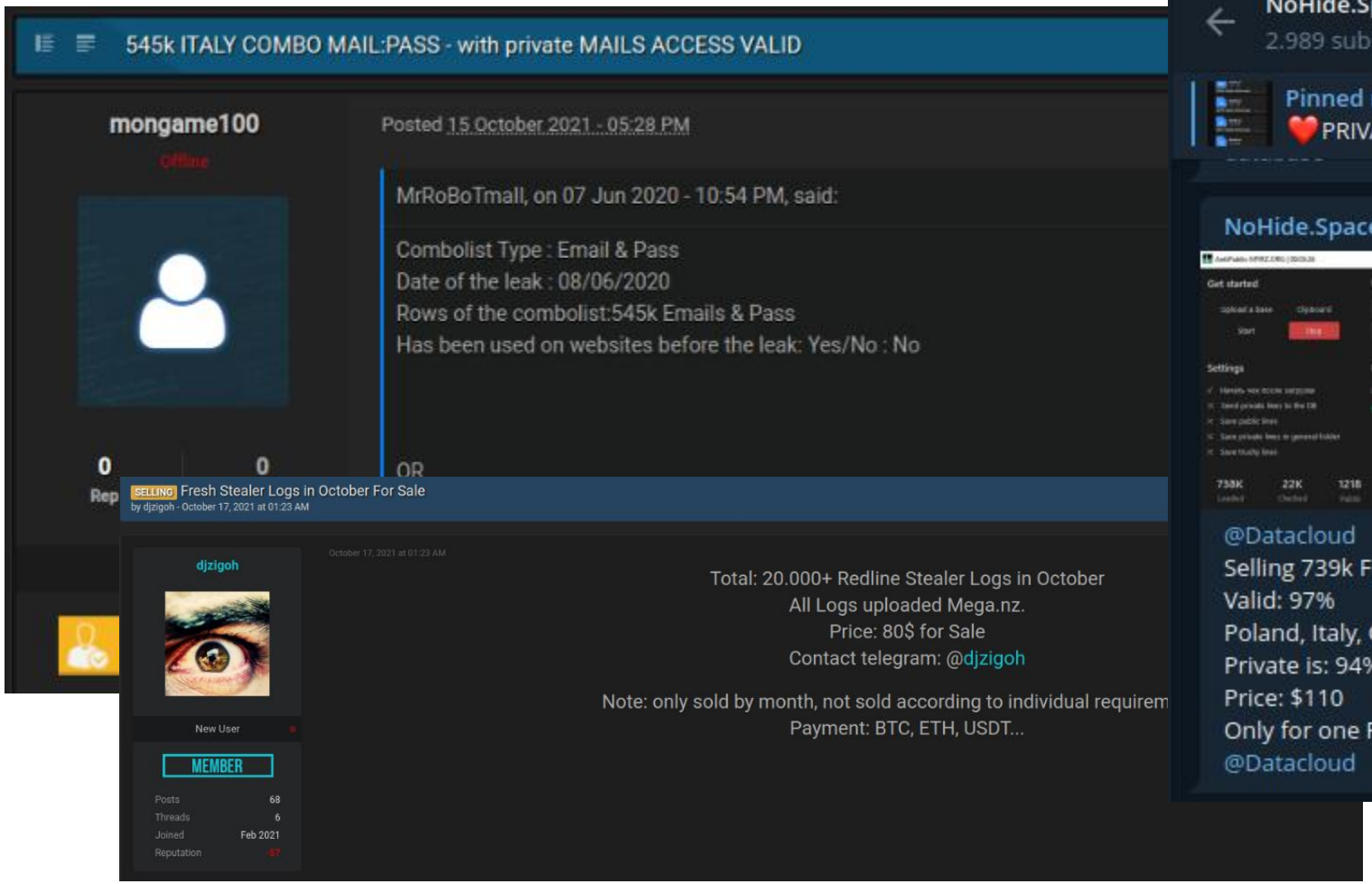
Malware – maggio 2024

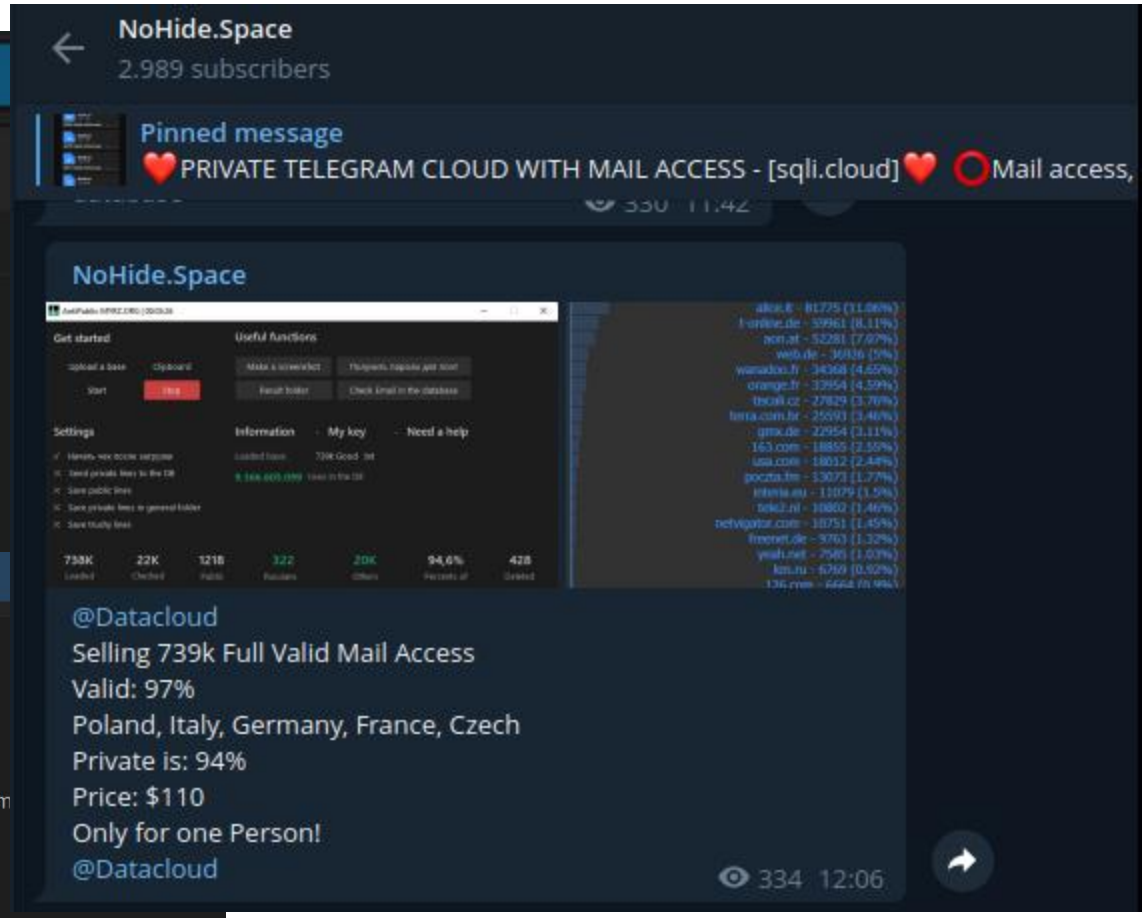
Campagne malevole



Compravendita di credenziali di accesso

Initial Access Broker





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
" Stealer
"Loader
" Ransomware
"E altri software

Contatti Jabber:
* Principale: hellxss@thesecure.biz (otr)
* Riserva: tox
* Telegram: non uso
Senza OTR , non scrivermi nemmeno...
Verificare immediatamente tramite il PM.

Пишу кода на c, c++, php, nod
Пишу практически все и завис
» Malware
» Stealer
» Loader
» Ransomware
» И другой софт

Джаббер контакты:
* Основная: hellxss@thesecure
* Резерв: tox
* Telegram: не использую

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

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

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

Feature List

Removal of backups
Hybrid RSA AES-256 encryption
UAC bypass
Sandbox Detection
Evasion of heuristic analysis
Heavy obfscuation
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 t
header.

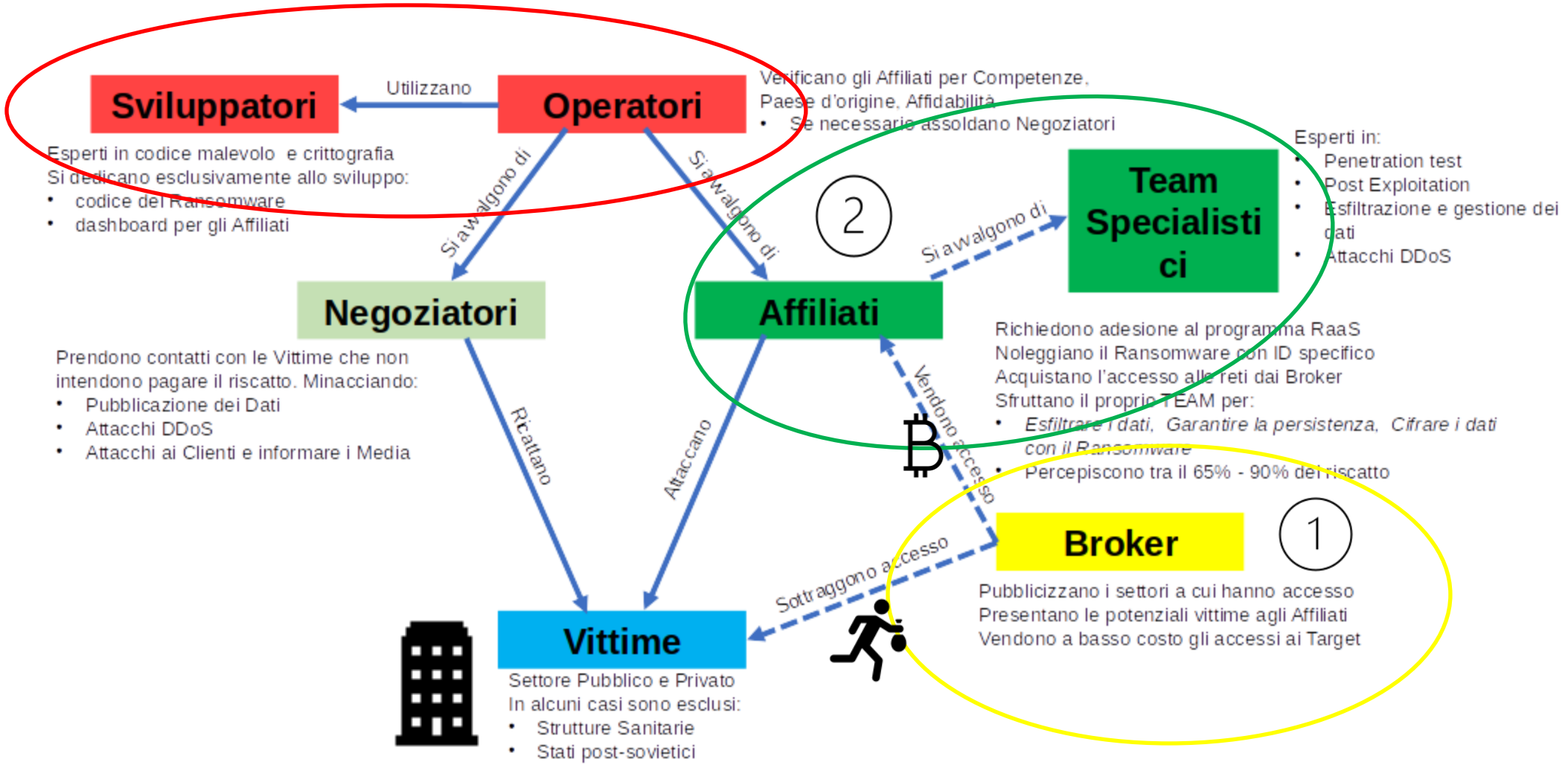
What you will recieve

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 tou recieve 100% of your ransoms! :)

Payload size is 2.7 MB

Galassia e organizzazione del Ransomware as a Service



Grazie per l’attenzione