Clusit
Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

SECURITY SUMMIT

Security Summit

Milano 19-20-21 marzo 2024

Sessione

Mauro Cicognini, Comitato Scientifico, Clusit

Marco Lucchina, Country Manager, Cynet

19 marzo 2024 orario 12.00

Mauro Cicognini

COMITATO
SCIENTIFICO
CLUSIT

Clusit
Associazione Italiana
per la Sicurezza Informatica

SECURITY SUMMIT

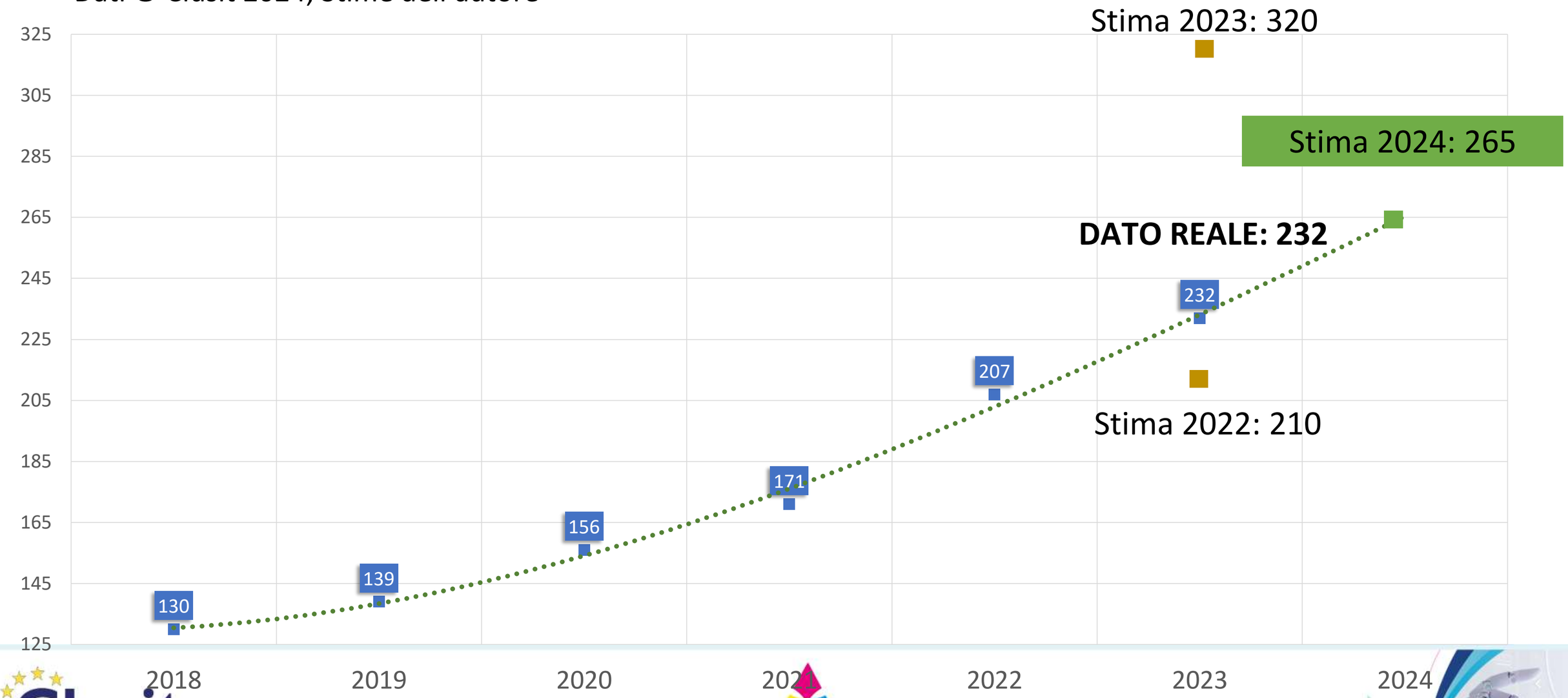
ASTREA Advanced Security, Training Research, Events Agency

Qualche nota positiva

- L’anno scorso sono stato troppo pessimista
  - Forse gli sforzi stanno iniziando a funzionare
- DORA è già in vigore, NIS 2 sarà pienamente operativo tra pochi mesi
- Il DMA ed il DSA stanno entrando in vigore
  - La Commissione Europea sta ospitando gli workshop con gli stakeholders in questi giorni
- L’AI è una grande opportunità

2024: Media mensile degli incidenti gravi

Dati © Clusit 2024; Stime dell'autore



Marco Lucchina

COUNTRY MANAGER
ITALY, SPAIN AND PORTUGAL

cynet

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT

«Only 36% of successful attacks have been delivered thought malware»

Il ragionamento in negativo di ABRAHAM WALD

cynet

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT

MaaS

Nexus	Godfather	Pixpirate	Saderat	Hook	PixBankBot	Xenomorph v3	Vultur	BrasDex	GoatRat
									
498 Known Variants	1,171 Known Variants	123 Known Variants	300 Known Variants	14 Known Variants	4 Known Variants	6 Known Variants	9 Known Variants	1 Known Variants	52 Known Variants
39 Banking Apps Targeted	237 Banking Apps Targeted	10 Banking Apps Targeted	8 Banking Apps Targeted	468 Banking Apps Targeted	4 Banking Apps Targeted	83 Banking Apps Targeted	122 Banking Apps Targeted	8 Banking Apps Targeted	6 Banking Apps Targeted
9 Countries Targeted	57 Countries Targeted	1 Countries Targeted	23 Countries Targeted	43 Countries Targeted	1 Countries Targeted	14 Countries Targeted	15 Countries Targeted	1 Countries Targeted	1 Countries Targeted
Offered as MaaS	Offered as MaaS	Not offered as MaaS	Not offered as MaaS	Offered as MaaS	Not offered as MaaS	Offered as MaaS	Not offered as MaaS	Not offered as MaaS	Not offered as MaaS
Stolen Data Exfiltrated to: USA, Netherlands, Turkey, Spain	Stolen Data Exfiltrated to: USA, Turkey, Spain, Canada, France, Germany, UK, Italy, Poland	Stolen Data Exfiltrated to: Brazil	Stolen Data Exfiltrated to: Thailand, Philippines, Peru	Stolen Data Exfiltrated to: Russia	Stolen Data Exfiltrated to: Brazil	Stolen Data Exfiltrated to: USA	Stolen Data Exfiltrated to: USA	Stolen Data Exfiltrated to: Australia, Poland	Stolen Data Exfiltrated to: Brazil

cynet

Cloud9: Chrome Extension Enables Remote Device Control

Late in the fall of 2022, the zLabs team discovered a malicious, potentially extremely dangerous extension to the Chrome browser. Dubbed Cloud9, this malware has the ability to steal information available during browser sessions. In addition, it can install malware that enables malicious actors to gain control over the infected device. This malware is distributed in a number of ways, including sideloading through fake executables and malicious websites purporting to provide users with Adobe Flash Player updates.

Schoolyard Bully: Trojan Credential Stealer Afflicts 300,000 Victims

Late in 2022, zLabs discovered a new Android threat campaign, the Schoolyard Bully Trojan. These trojans have been found in numerous apps that were downloaded from the Google Play Store and third-party app stores. The trojans are hidden within seemingly legitimate educational apps. Claiming more than 300,000 victims, the malware is focused on stealing an individual's Facebook credentials. While these malicious apps have been removed from the Google Play store, they remain on numerous third-party app sites.

TeaBot campaign. TeaBot is a banking trojan that was first detected by Cleafy in 2021.[9] This malware is designed to steal victims' credentials and SMS messages. In late 2021 and early 2022, the number of malware samples grew substantially. Ultimately, more than 400 malicious apps were detected.

Dark Herring campaign. Early in 2022, Zimperium discovered this malware campaign which successfully targeted more than 105,000,000 victims around the world.[10] This campaign exploits direct carrier billing to scam money from unsuspecting users, and losses are estimated to have reached hundreds of millions of dollars.

RatMilad campaign. In the fall of 2022, the Zimperium zLabs team issued a warning about RatMilad, an Android spyware campaign targeting individuals in the Middle East.[11] The spyware was hidden within a phone number spoofing app and was distributed under the guise of enabling users to independently verify a social media account. Once users installed the app, malicious actors could gain control over their mobile devices, including the ability to view contacts, phone call logs, media, and files.

Dirty RatMilad: Android Spyware

Mobile spyware is no longer just the domain of sophisticated government surveillance teams and nation states. RatMilad is just one example of how this type of spyware is being employed by smaller organizations. This malware (which has various spyware capabilities such as data exfiltration techniques) has taken various forms. The original variant of RatMilad was hidden within a phone number spoofing app called Text Me, an app that purported to help users verify a social media account by phone. In the fall of 2022, zLabs discovered a live sample of RatMilad hidden within an app called NumRent, which is a renamed, updated version of Text Me. These apps are distributed through links in messages and social media posts.

Dark Herring: Scamware Exceeds 100 Million Installations

Last year's report featured an Android Trojan attack known as GriftHorse, outlining how it infected 10 million devices in over 70 countries. Unfortunately, since that time, the scamware threat only became more widespread. Early in 2022, zLabs discovered Dark Herring, another scamware campaign. Dark Herring has targeted more than 100 million victims globally. This campaign exploits direct carrier billing to scam money from unsuspecting users, with losses estimated to have reached hundreds of millions of dollars.

MoneyMonger: Malware Disguised by Flutter

Near the end of 2022, zLabs announced the discovery of MoneyMonger. Disguised as an app enabling individuals to get loans, this malware campaign enables malicious actors to steal private data. MoneyMonger was discovered in a Flutter app. Flutter is an open-source software kit for developing cross-platform apps. Through Flutter, teams can develop and maintain one codebase while delivering native mobile apps on multiple device platforms. By taking advantage of Flutter's framework, the threat actors behind MoneyMonger were able to obfuscate malicious features so they're not detected by legacy mobile security products.

The Godfather

- Anti-emulator
- Collect victim's device info
- Unstructured Supplementary Service Data
- Call forwarding
- Push notifications
- Smishing
- Steal SMSs
- Record the screen
- VNC
- Start/Kill the malware
- Cache cleaner

Raccon stealer

Cost: 75-200 per month

Cryptocurrency Exodus, Monero, Jaxx, Binance

Passwordmanager: Bitwarden, 1Password, and LastPass

Email clients: Outlook, ThunderBird, and Foxmail

Others: Steam Authorisation or Steam Sentry File - Telegram

Info-stealer market

Infostealer LOGs: + 150% every two months*

Infostealers can easily be installed on a computer or device via phishing, infected websites, malicious software downloads and Google ads. A log represents the complete collection of assets that can be stolen from a victim's endpoint, from cookies through to stored credentials

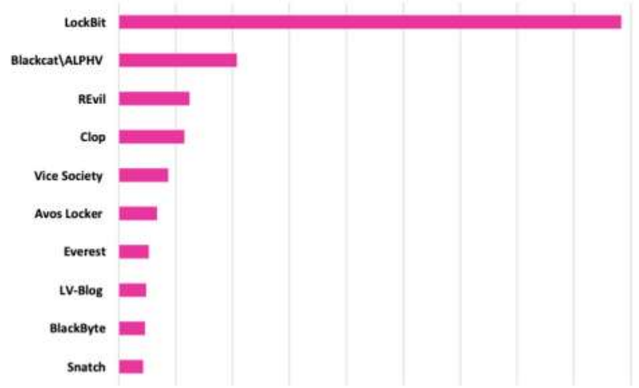
- **Raccoon**: 2,114,549
- **Vidar**: 1,816, 800
- **Redline**: 1,415,458

```
URL: https://vpn.[redacted].com/+CSCOE+/logon.html
Username: [redacted]
Password: [redacted]
Application: Google_[Chrome]_Default

URL: https://mail.[redacted]/owa/auth/logon.aspx
Username: [redacted]
Password: [redacted]
Application: BraveSoftware_[Brave-Browser]_Default

[Line]  URL: https://[redacted].salesforce.com/
Username: [redacted]
Password: [redacted]

Soft: Google Chrome [Default]
Host: https://rds.[redacted].com/RDWeb/Pages/fr-FR/login.aspx
Login: re[redacted]
Password: [redacted]

SOFT: Chrome (v109.0.5414.75-64, Profile: Default)
URL: https://intranet.[redacted].it/
USER: [redacted]
PASS: [redacted]

SOFT: Chrome (v112.0.5615.49-64, Profile: Default)
URL: https://exchange.[redacted].sg/passwordportal/
USER: [redacted]
PASS: [redacted]
```

cynet

Something is changing

- Qakbot: 700k+ host infected (Botnet)
- Genesis market: 1,5M+ host infected (credentials)
- Raid forum: 800M+ records
- Russian market: Genesys+Raid
- ChatGPT/Bard ha un ritorno 20 volte superiore per ogni campagna PHISHING. Ogni 500000 email inviate si stima un ritorno di 2+ milioni di $.
- Ransomware: +63% di riscatti pagati a fronte di una diminuzione del valore medio.
- Attacchi mensili: +53%
- Affiliate program: +200%
- Adavanced tactics and technics: 138 ATP groups



cynet

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT

Cybercrime business models

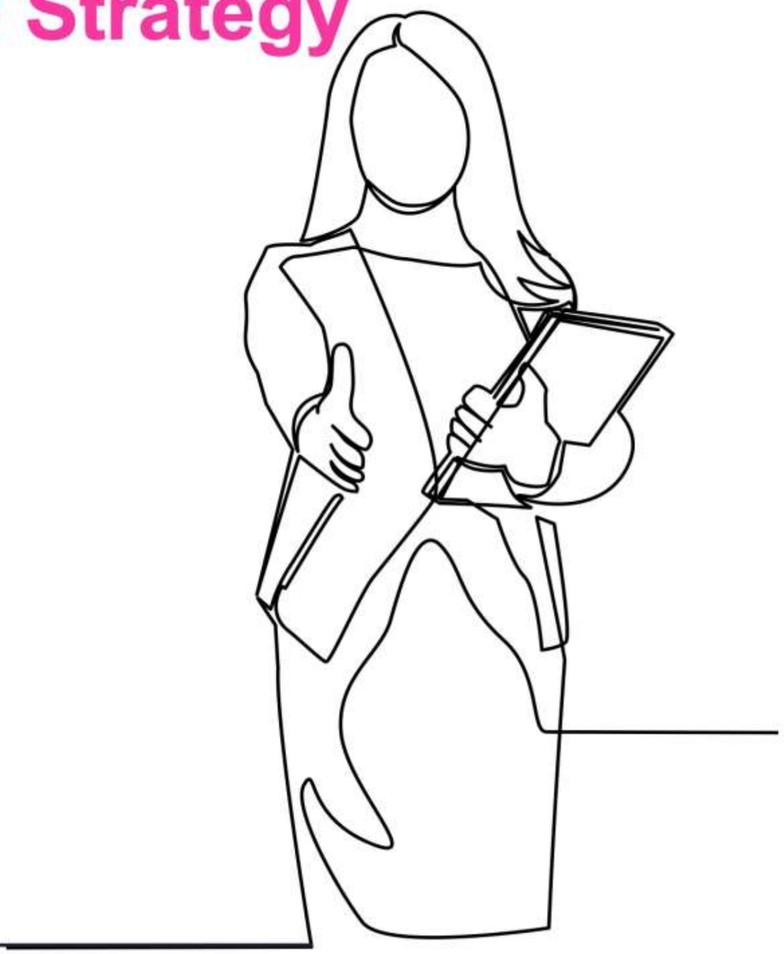
cynet

Extended Defense & Response Strategy

VISIBILITY everywhere data are stored,
FORENSICS analysis

POLICY enforcement, POSTURE
monitoring, detection of TTPs

PLAYBOOKS & INCIDENT RESPONSE
protocols



cynet

cynet

Clusit
Associazione Italiana
per la Sicurezza Informatica

SECURITY SUMMIT

See you soon.

Cynet's stand for a (real) presentation, demo, discussion and gadgets

cynet

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT

Q&A

VIENI A TROVARCI AL NOSTRO STAND!

CONTATTI:

XXXXXXXXX