Cybersecurity: riguarda anche noi?

28 Aprile 2021

Mauro Cicognini
Membro del Comitato Direttivo, CLUSIT

Clusit

L'INDUSTRIA DELLA GOMMA

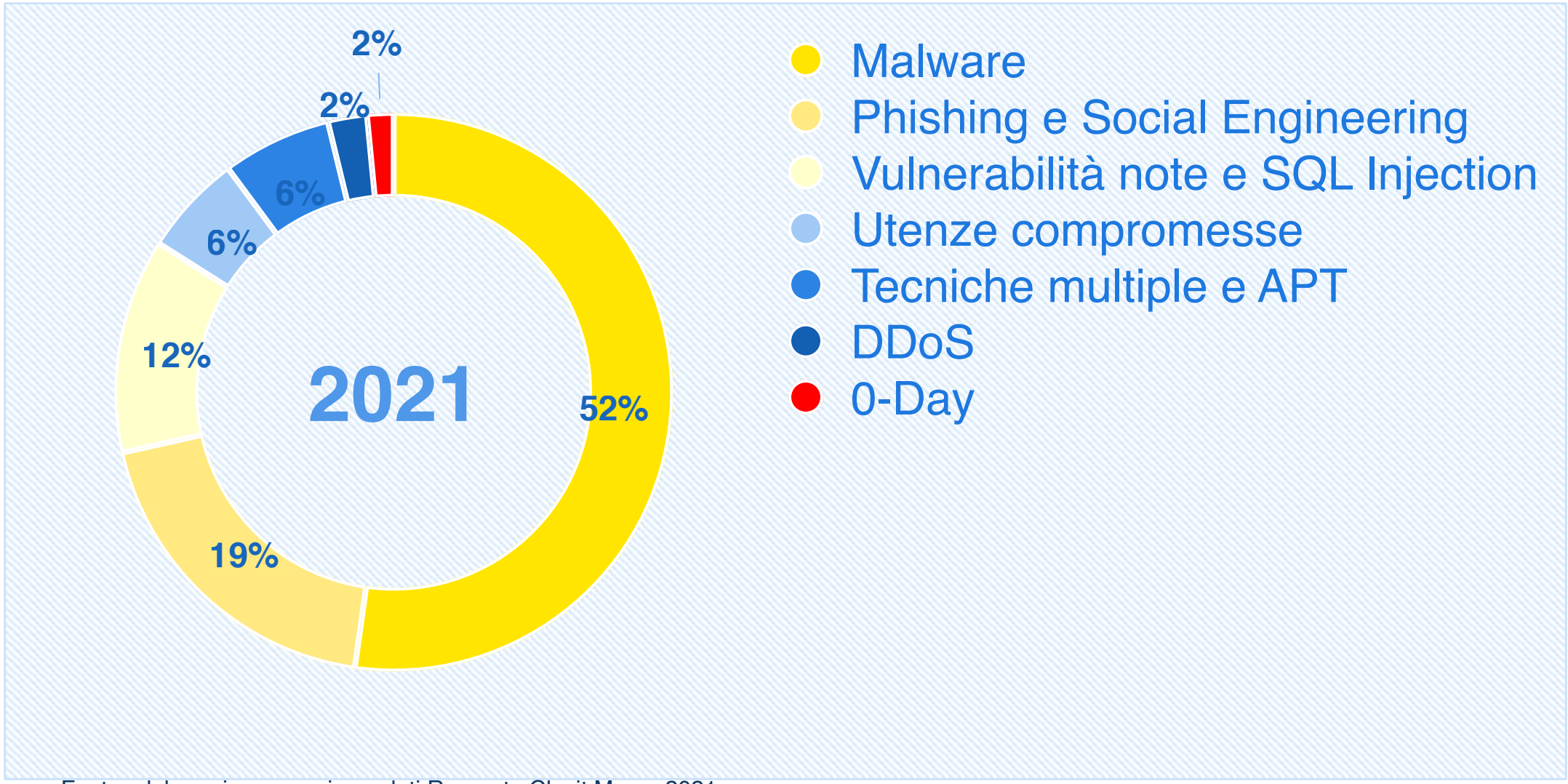
Clusit – Associazione Italiana per la Sicurezza Informatica

- Nasce nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano
- Rappresenta sia oltre 500 organizzazioni, appartenenti a tutti i settori del Sistema-Paese, sia numerosi soci individuali
- Gli obiettivi:
  - Diffondere la cultura della cybersecurity
  - Promuovere l'uso di tecnologie e metodologie per rendere più sicure aziende e PA
  - Contribuire alla formazione dei singoli e delle organizzazioni sia con eventi, seminari ed altre iniziative, sia partecipando alla stesura degli standard di certificazione
  - Collaborare con le istituzioni nazionali ed europee e partecipare all'elaborazione di leggi e regolamenti di settore

Le attività principali:

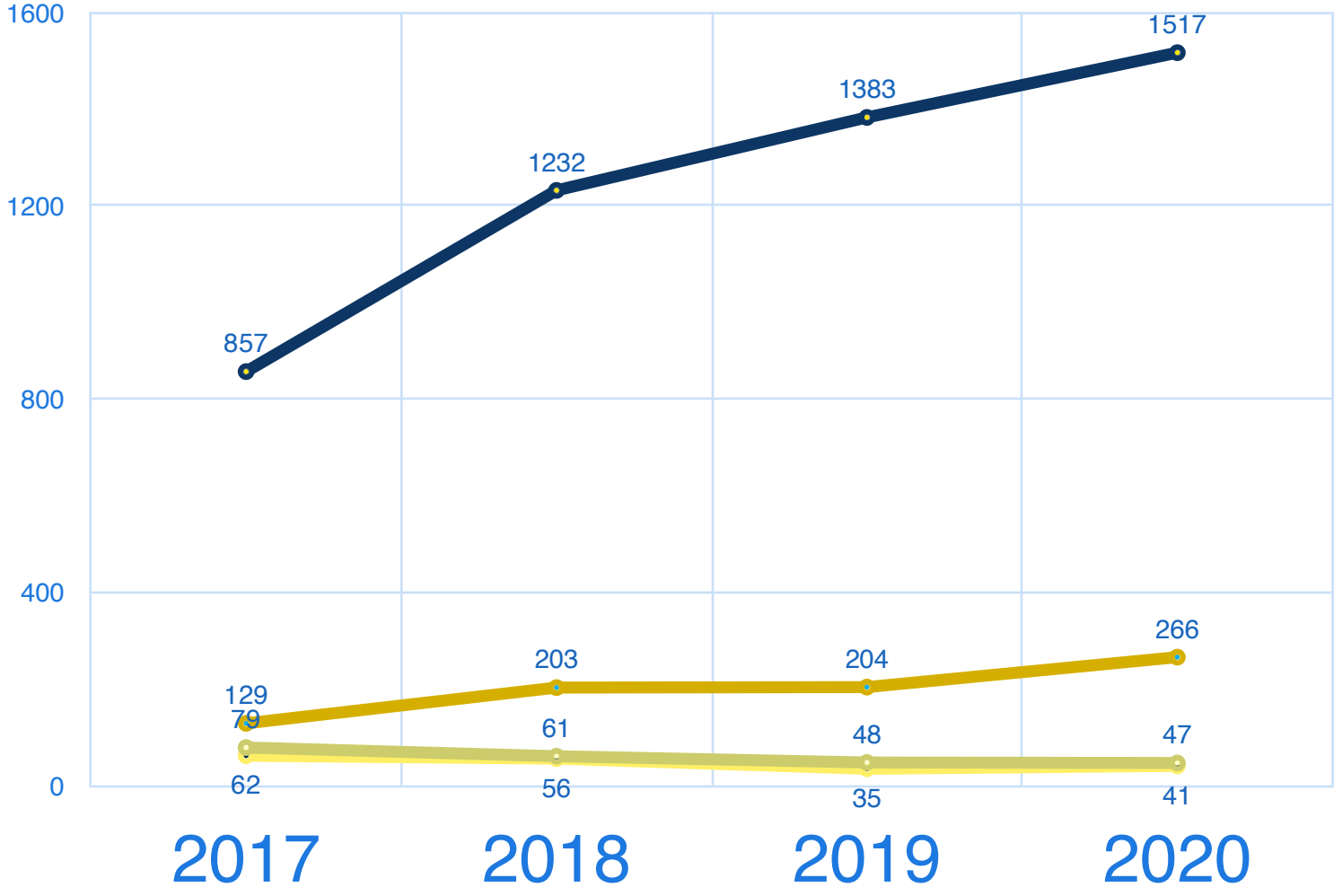
- Il Security Summit www.securitysummit.it
- Gli Atelier del Security Summit (in streaming)
- L'annuale *Rapporto Clusit* sullo stato della cybersecurity in Italia
- Sponsorizzazione della Community for Security e di gruppi di lavoro su vari temi
- Produzione di documenti tecnico-scientifici

Tecniche di attacco note (dati fino a febbraio 2021)

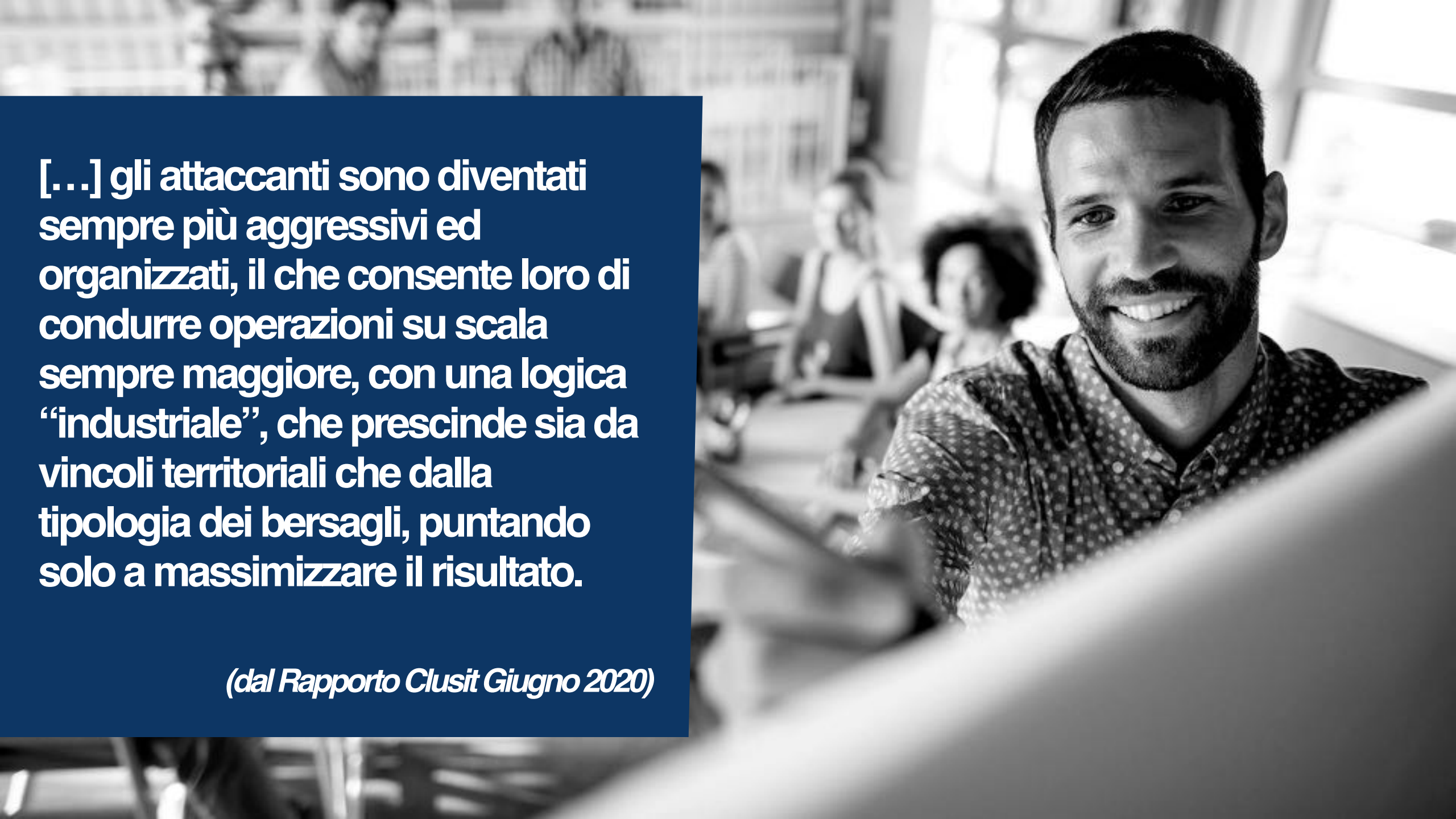


Fonte: elaborazione propria su dati Rapporto Clusit Marzo 2021

Qual è il fine degli attacchi?



Fonte: elaborazione propria su dati Rapporto Clusit Marzo 2021



[…] gli attaccanti sono diventati sempre più aggressivi ed organizzati, il che consente loro di condurre operazioni su scala sempre maggiore, con una logica "industriale", che prescinde sia da vincoli territoriali che dalla tipologia dei bersagli, puntando solo a massimizzare il risultato.

(dal Rapporto Clusit Giugno 2020)

CORRIERE DELLA SERA

BRESCIA / ECONOMIA

CYBERSECURITY

Attacco hacker al Comune di Brescia: «I dati rubati sono già in rete. Così funziona il ricatto online»

Dedola (Kaspersky): il gruppo DoppelPaymer potrebbe girarli a terzi. Il Comune aveva invece assicurato che non c'era stata alcuna fuoriuscita di informazioni. Si apre il caso

di Massimiliano Del Barba

A oltre due settimane dalla notte del 30 marzo, sono ancora tanti i contorni non ancora ben definiti circa le motivazioni e i reali danni dell'attacco hacker scagliato contro l'infrastruttura informatica del Comune di Brescia. «Cominciamo col dire che **Brescia non è l'unica pubblica amministrazione che è stata oggetto di un ransomware in questi giorni**: sarle analoga l'hanno avuta le architetture IT di Rho e di Caselle Torinese, in Piemonte» dice **Giampaolo Dedola, Senior Security Researcher del GReAT Team di Kaspersky**, società russa con sede a Mosca fondata nel 1997 da Evgenij Kasperskij e specializzata in sistemi di sicurezza informatica. (leggi qui il riassunto della vicenda)

Perché Brescia?

«Per soldi. Si tratta di gruppi criminali, che magari non sono al corrente del fatto che le amministrazioni pubbliche italiane non possono pagare riscatti. Municipalità e Comuni vengono attaccati con regolarità in tutto il mondo. Le modalità sono tipiche: trovano uno spiraglio e poi si diffondono nell'infrastruttura per prenderne il controllo».

Un ransomware per il Comune di Brescia

- Incidente venuto alla luce alla fine di marzo 2021
- Il primo sintomo che ho visto di persona è stato un messaggio email che ha "rimbalzato" il 5 aprile
  - Il destinatario era un indirizzo istituzionale, quindi è stato subito chiaro che c'era un problema abbastanza grave
- Tutti i servizi del Comune sono rimasti indisponibili per molte ore, poi hanno ripreso a singhiozzo
- Ad oggi non c'è alcuna certezza che i dati del Comune (pratiche edilizie, ecc.) siano rimasti integri
- Comunicazione gestita maluccio…
  - "Siamo *quasi* certi che nessun dato sia uscito dal Comune" (il corsivo è mio)
- https://brescia.corriere.it/notizie/economia/21_aprile_16/attacco-hacker-comune-brescia-dati-rubati-sono-gia-rete-cosi-funziona-ricatto-online-ce99ca2a-9e8a-11eb-a475-be5cae54c7bb.shtml

Un ransomware per il mio carrozziere

- Evento del 2016: scarica inavvertitamente un ransomware, che in brevissimo tempo cifra interamente il contenuto dei 3 PC nell'ufficio
- Riscatto richiesto: 0,99 BTC, all'epoca poche centinaia di euro
  - Oggi sarebbero circa €45.000
- Backup: inservibile → decide di pagare
- Ha rapidamente imparato come installare Tor e farsi un borsellino in bitcoin
- E' stato fortunato: ha trovato un ladro onesto, che gli ha fornito le chiavi di decifratura

Per sintetizzare:

Gli attacchi informatici fanno parte della quotidianità; dobbiamo convivere con essi

Vanno trattati come qualcosa che può succedere a prescindere dai nostri sforzi

La strategia è necessariamente complessa e coinvolge persone, processi, e tecnologie

Prevenzione per quanto possibile, e contromisure per quando qualcosa, malauguratamente, va storto

Q & A

Grazie per l’attenzione!