oapoint

L’Evoluzione dell’IT nell’era del Cyber Crime

TAVELLAW STUDIO DI AVVOCATI

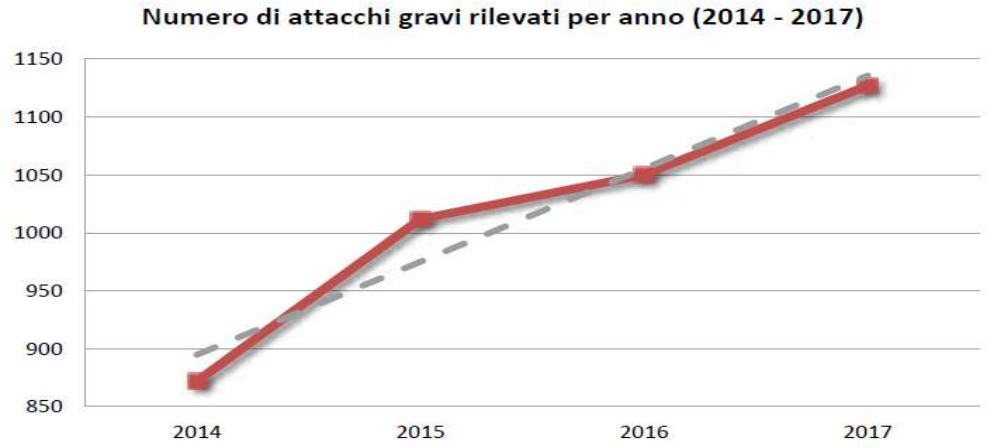
KASPERSKY lab

WatchGuard

VEEAM

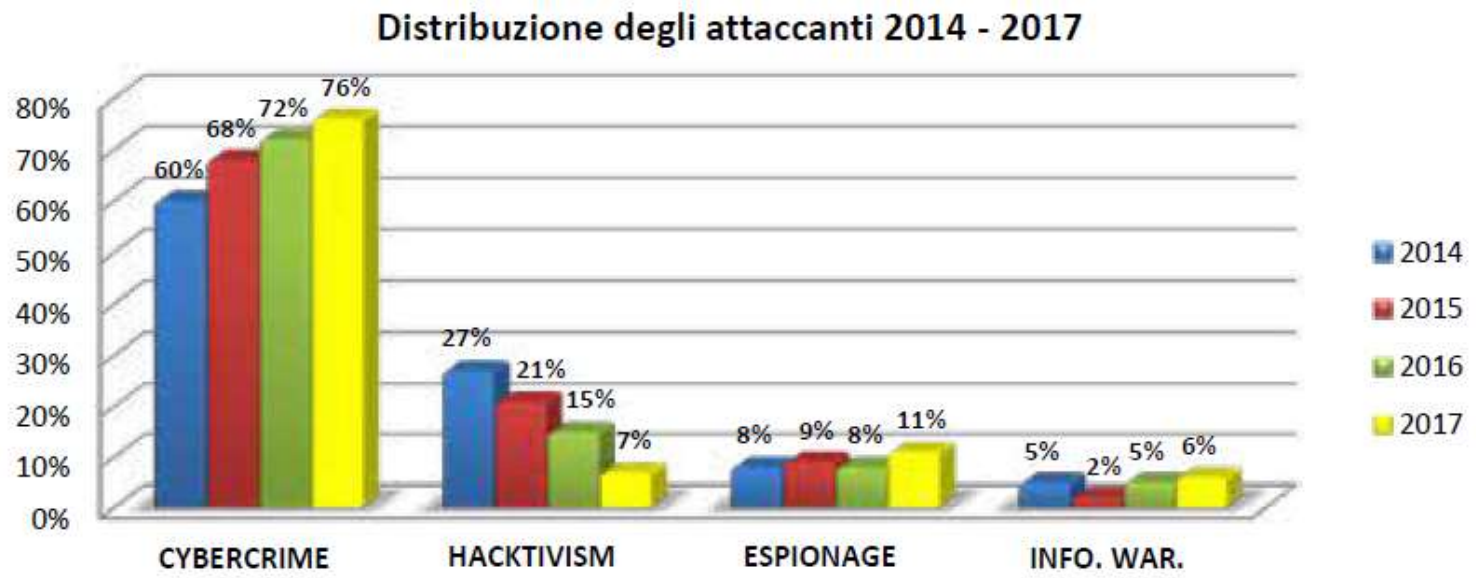
13-15 Marzo 2018 Security Summit - Rapporto del CLUSIT, Associazione Italiana per la Sicurezza Italiana: https://clusit.it/rapporto-clusit/

L'analisi è basata sulla valutazione di tutte le informazioni pubblicamente disponibili in merito a un campione di attacchi "gravi" che è costituito da oltre 1.100 incidenti noti avvenuti tra il gennaio 2014 e il dicembre 2017.



© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia

In particolare sono certamente meglio rappresentati gli attacchi realizzati per finalità cyber criminali o di hacktivism rispetto a quelli derivanti da attività di cyber espionage e information warfare, più sommersi.



oapoint

Distribuzione degli attaccanti per tipologia

ATTACCANTI PER TIPOLOGIA	2014	2015	2016	2017	Variazioni 2017 su 2016	Trend 2017
Cybercrime	526	684	751	857	14,11%	
Hacktivism	236	209	161	79	-50,93%	
Espionage / Sabotage	69	96	88	129	46,59%	
Information Warfare	42	23	50	62	24,00%	
TOTALE	873	1.012	1.050	1.127	+7,33%	

TAVELLA LAW STUDIO DI AVVOCATI

KASPERSKY lab

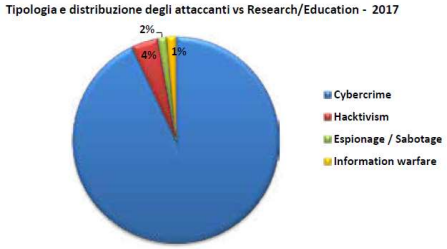
WatchGuard

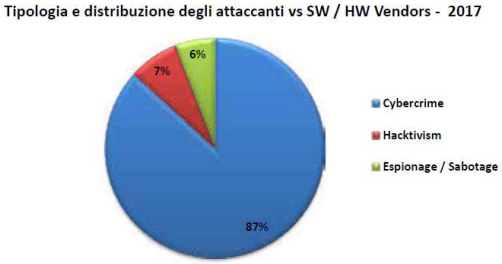
VEEAM

oapoint

Distribuzione degli attaccanti per le categorie a maggior tasso di crescita degli attacchi

Quest'anno le categorie che mostrano il maggiore tasso di crescita degli attacchi rispetto all'anno precedente sono:
Multiple Targets +353% Research/Education +29% Software/Hardware Vendors +21%





TAVELLA LAW STUDIO DI AVVOCATI KASPERSKY lab WatchGuard VEEAM

Distribuzione generale delle vittime per tipologia

VITTIME PER TIPOLOGIA	2014	2015	2016	2017	Variazioni 2017 su 2016	Trend 2017
Institutions: Gov - Mil - LEAs - Intelligence	213	223	220	179	-18,64%	↓
Others	172	51	38	40	5,26%	↗
Entertainment / News	77	138	131	115	-12,21%	↘
Online Services / Cloud	103	187	179	95	-46,93%	↓
Research - Education	54	82	55	71	29,09%	↑
Banking / Finance	50	64	105	117	11,43%	↑
Software / Hardware Vendor	44	55	56	68	21,43%	↑
Telco	18	18	14	13	-7,14%	↘
Gov. Contractors / Consulting	13	8	7	6	-14,29%	↘
Security Industry	2	3	0	11	-	↗
Religion	7	5	6	0	-	↓
Health	32	36	73	80	9,59%	↑
Chemical	5	2	0	0	-	→
Critical Infrastructures	13	33	38	40	5,26%	↗
Automotive	3	5	4	4	-	→
Org / ONG	47	46	13	8	-38,46%	↓
Multiple Targets	-	-	49	222	353,06%	↑
GDO / Retail	20	17	29	24	-17,24%	↘
Hospitability	-	39	33	34	3,03%	↗

oapoint

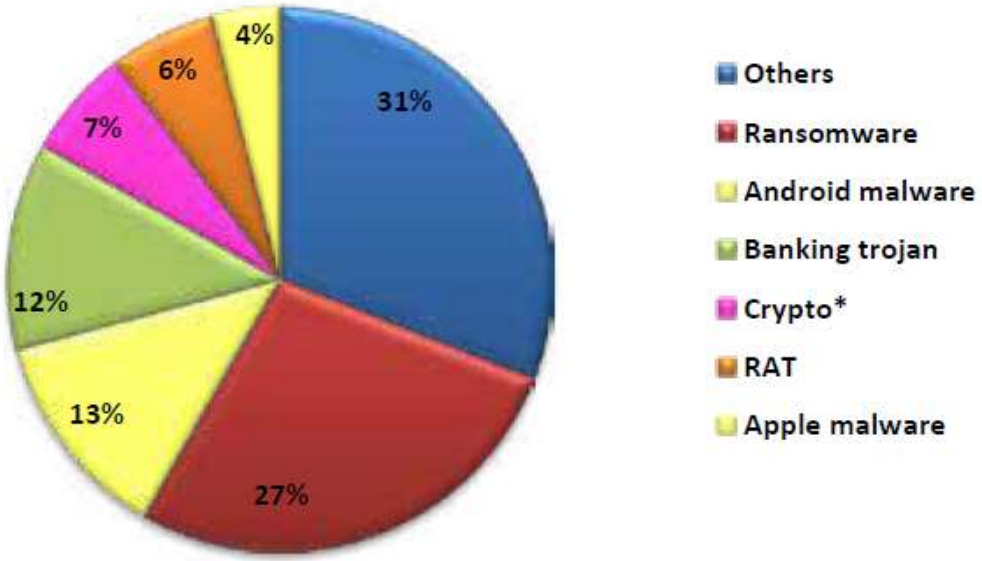
Distribuzione delle tecniche di attacco

TECNICHE DI ATTACCO PER TIPOLOGIA	2014	2015	2016	2017	Variazioni 2017 su 2016	Trend 2017
SQL Injection	110	184	35	7	-80,00%	↓
Unknown	199	232	338	277	-18,05%	↓
DDoS	81	101	115	38	-66,96%	↓
Known Vulnerabilities / Misconfigurations	195	184	136	127	-6,62%	↘
Malware	127	106	229	446	94,76%	↑
Account Cracking	86	91	46	52	13,04%	↗
Phishing / Social Engineering	4	6	76	102	34,21%	↑
Multiple Techniques / APT	60	104	59	63	6,78%	↗
0-day	8	3	13	12	-7,69%	↘
Phone Hacking	3	1	3	3	-	→

TAVELLA LAW STUDIO DI AVVOCATI KASPERSKY lab WatchGuard VEEAM

oapoint

Tipologia Malware - 2017



TAVELLA LAW STUDIO DI AVVOCATI

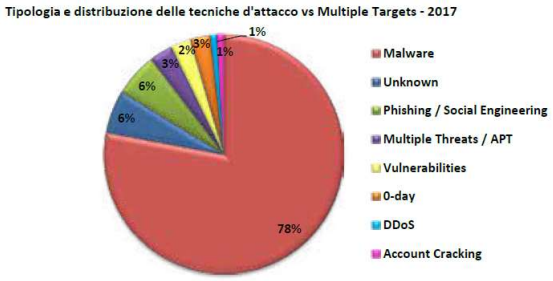
KASPERSKY lab

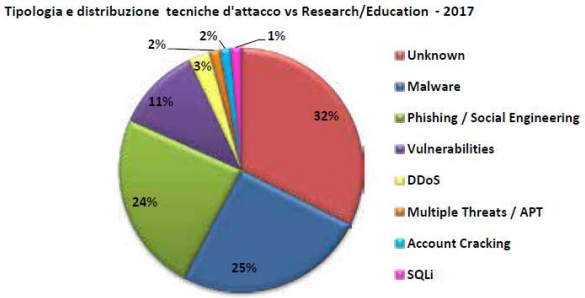
WatchGuard

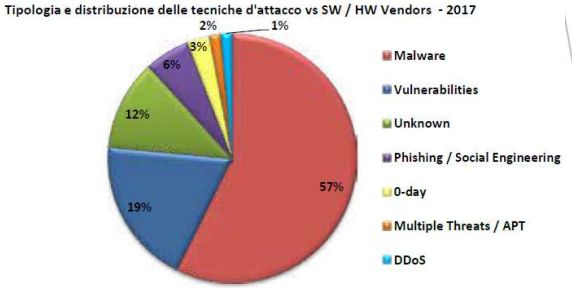
VEEAM

oapoint

Distribuzione delle tecniche di attacco utilizzate verso le vittime di categorie a maggior tasso di crescita degli attacchi:







TAVELLAW STUDIO DI AVVOCATI

KASPERSKY lab

WatchGuard

VEEAM

Se dovessimo riassumere in tre concetti-chiave la situazione, potremmo dire che il 2017 si è caratterizzato come “l’anno del trionfo del Malware, degli attacchi industrializzati realizzati su scala planetaria contro bersagli multipli e della definitiva discesa in campo degli Stati come attori di minaccia” per cui ricordiamo tra tutti:

- le interferenze durante le campagne presidenziali americana e francese;
- gli attacchi realizzati tramite centinaia di migliaia di device IoT compromessi;
- gli attacchi con finalità geopolitiche basati sui malware WannaCry e NotPetya;
- i numerosi data breach che hanno coinvolto complessivamente miliardi di account.

Il livello degli attaccanti si sta evolvendo e strutturando: questa nota deve essere presa in considerazione con molta attenzione.

E quindi?

Quindi arriva Il regolamento generale Europeo sulla protezione dei dati (GDPR, General Data Protection Regulation - Regolamento UE 2016/679).

Il Regolamento UE porta un'impostazione «sistemica»: Il tema della sicurezza passa da una logica di «minimo» a una logica di «adeguato» in base ai rischi corsi (e nei casi previsti alla valutazione di impatto).

Non è una Rivoluzione, è una semplice Evoluzione: evoluzione del Sistema Informativo, responsabilizzazione personale, impegno nella formazione.

oapoint

Alcuni punti di verifica:

1) Compilazione del Registro dei Trattamenti
2) Security & Risk Assessment
3) Documento di Valutazione di Impatto
4) Gestione dei Data Breach
5) Redazione, pubblicazione e formazione su Policy & Procedure
6) Gestione contratti di fornitura
7) Revisione informative agli interessati
8) Applicazione procedure per i diritti dell'interessato all'oblio
9) Revisionare la gestione del consenso
10) Preparazione procedure comunicazioni con il Garante
11) Preparazione procedure comunicazioni violazione dati agli Interessati
12) Adozione misure di Sicurezza aggiuntive rispetto alla situazione precedente all'approvazione del GDPR

TAVELLA AW STUDIO DI AVVOCATI KASPERSKY lab WatchGuard VEEAM

oapoint

Preoccupazioni legittime	Benefici collaterali
➢ Gravi sanzioni	✓ Maggiore sicurezza dei dati
➢ Costretti a investire per la conformita`, anziche' per necessità strategiche, commerciali, tecnologiche	✓ Evita perdite finanziarie ed economiche
➢ Grave rischio per l'immagine in caso di compromissione	✓ Previene problemi di reputazione, migliora l'immagine aziendale
➢ Impatto negativo su vendite, marketing , relazioni clienti, trattamento dati, outsourcing, cloud, etc	✓ Stimola investitori e partner
➢ Impatto negativo sulle relazioni aziendali e sul controllo dei dipendenti	✓ Contrasta il traffico illegale di dati
	✓ Benefici anche per la protezione del resto dell'informazione (Proprieta` Intellettuale...)
	✓ Rompe i silo tra divisioni aziendali
	✓ Snellisce processi e dati
	✓ I consumatori pretendono piu` sicurezza e privacy per i propri dati personali.

TAVELLAW STUDIO DI AVVOCATI KASPERSKY lab WatchGuard VEEAM

oapoint

Evoluzione dell'IT, non Rivoluzione.

Abbiamo l'opportunità di sfruttare un Regolamento Europeo che permette di rimettere al centro l'individuo cercando di riportare l'attenzione sulla responsabilità derivante dal possedere informazioni (dati) per cercare di elevare i livelli di diritto, libertà e tutela.

Abbiamo il dovere di elevare il livello di Sicurezza del nostro Sistema Informativo e l'offerta Tecnologica di consente di poter trovare la miglior soluzione per coprire esigenze specifiche tra cui:

- Firewall (periferici e moduli IPS interni);
- Sistemi AntiSpam e SandBox
- Ambienti SIEM
- Protezioni End Point
- Gestione del dato (sistemi di backup)

TAVELLAW STUDIO DI AVVOCATI KASPERSKY lab WatchGuard VEEAM