

# Darkbox®

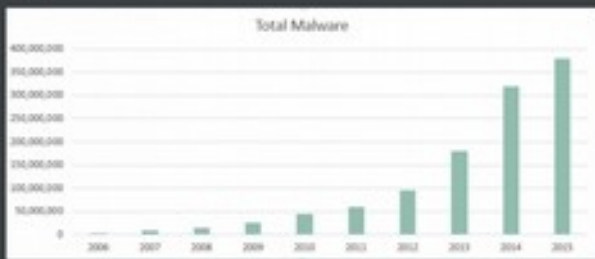
Network monitoring > Increase security > GDPR ready



Presentazione prodotto

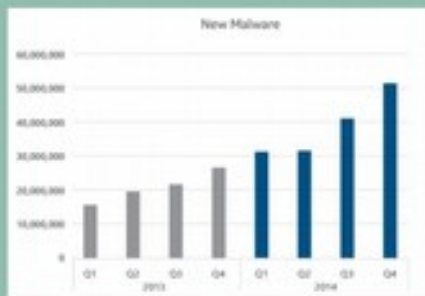
Settembre 2020

## THE PROLIFERATION OF MALWARE SINCE 2006

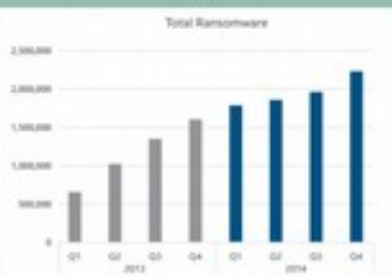


The rate at which Malware is proliferating has been increasing drastically over the past ten years, with the total number of malware instances expected to number more than 400 million by the end of 2015. From 2012 through 2014, the total number of malware instances more than tripled.

**387 NEW MALWARE THREATS EVERY MINUTE in 2014**



In 2014, there were over 50,000,000 new instances of malware. This amounted to over 387 new threats every minute or more than 6 every second!



**OVER 2 MILLION "RANSOMWARE" THREATS HAVE BEEN DETECTED**

"Ransomware," or malware attacks where information is held for ransom, have been on a rapid rise in the past two years. In Q4 of 2014, over 250,000 new instances of "ransomware" attacks were reported.

**60% OF FOUND USB THUMB DRIVES WERE PLUGGED IN**

In 2011, the U.S. Department of Homeland Security (DHS) planted computer discs, CDs and USB thumb drives in the parking lots around the DHS office to test the potential vulnerability posed by mobile media. The DHS found that 60% of people who picked up the devices plugged them in to a computer. Of those that found media planted with a DHS logo, 90% of the devices were plugged in to a computer.



# Perché Darkbox® ?

## Perché antivirus o firewall non bastano più

Darkbox risponde all'aumentato bisogno di cybersecurity

Darkbox risponde al bisogno di controllare e prevenire i rischi derivanti da fenomeni in costante aumento quali:

- PHISHING
- FRODI BANCARIE
- FURTO DI DATI e KNOW-HOW
- INTRUSIONE EMAIL
- ATTACCHI RANSOMWARE e criptaggi
- BITCOIN Mining

# Darkbox® è: GDPR Ready

## Articolo 32 del GDPR

- *[Il Titolare] mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio;*
- Le misure di prevenzione degli attacchi informatici prevedono un controllo di ciò che accade all'interno della propria rete
- Darkbox effettua il monitoraggio della LAN e segnala traffico anomalo da parte di qualsiasi dispositivo connesso.
- Utilizza software *open-source*



# Come funziona ?

Darkbox<sup>®</sup> è un sistema di monitoraggio di rete, basato sull'analisi dei pacchetti.

In una LAN PMI, agisce collegato allo switch principale.



Internet

Router

Firewall

Main Switch



Utenti della rete



EMAIL  
ALERTS

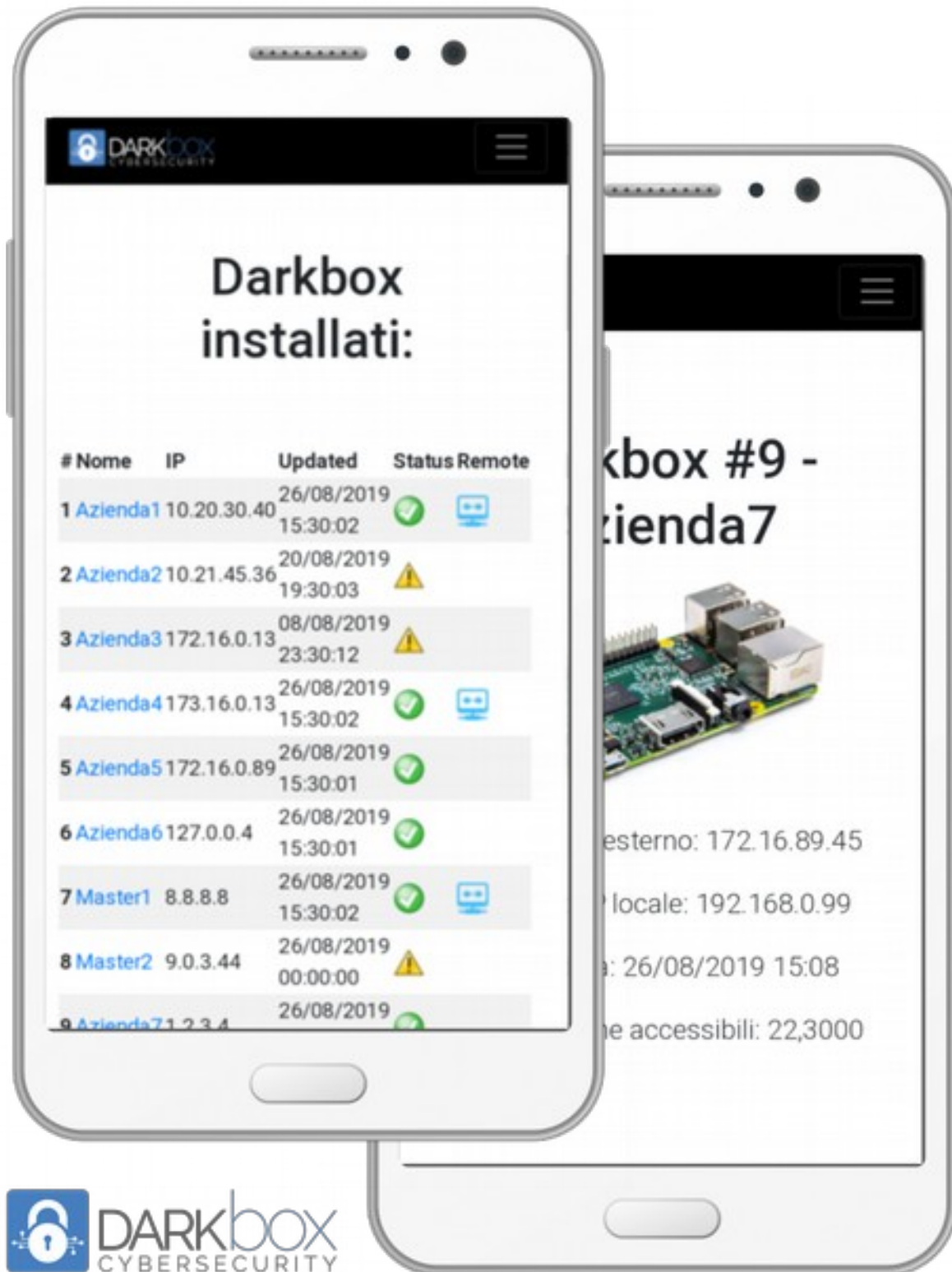


REGISTRO  
ATTIVITA'



LAN  
MONITORING

# Cosa può fare ?



- Stato di salute della rete
- Allarmi MALWARE
- Allarmi traffico anomalo da singoli IP
- Registra tutti i dispositivi che accedono
- Controlla traffico eccessivo
- Registra l'attività
- Trasmette allarmi via EMAIL

# Monitoraggio della rete

Scansione la rete locale e traccia tutti i dispositivi connessi

The screenshot displays two windows from the ntopng network monitoring application. The top window, titled "Discovered Devices", shows a table of detected network devices. The bottom window, titled "All Hosts", shows a detailed view of network flows and host statistics.

IP Address	Name	Manufacturer
192.168.1.107		
192.168.1.123		Sony Corporation [KDL-40W705C]
192.168.1.1		TP-LINK [TL-WR841N]
192.168.1.102		TP-Link Technologies Co.,Ltd.
192.168.1.113	EPSON XP-322 wifi @ HP-P552LA	Chicony Electronics Co., Ltd.
192.168.1.117		Raspberry Pi Foundation

	IP Address	Location	Flows	Alerts	Name	Seen Since	Breakdown	Throughput	Total Bytes
Flows	146.241.84.164	Remote Host	42	0	146.241.84.164	18:12	Sent Rcvd	3.7 kbit/s ↓	3.48 MB
Flows	10.0.0.98	Local Host	42	0	darkbox [darkbox]	3 days, 21:53:59	Sent Rcvd	3.7 kbit/s ↓	4.99 MB
Flows	10.0.0.97	Local Host	0	0	wdarkbox.homenet.telecomitalia...	3 days, 21:53:52	Sent	0 bit/s →	137.29 KB
Flows	10.0.0.254	Local Host	0	0	Linux.homenet.telecomitalia...	3 days, 09:29:24	Sent	0 bit/s →	1.84 MB
Flows	10.0.0.1	Local Host	1	0	modemtim.homenet.telecomitalia...	3 days, 21:53:59	Sent	95.98 bit/s ↑	2.0 MB

Showing 1 to 5 of 5 rows. Idle hosts not listed.

ntopng Community/Embedded Edition v.3.8.190204  
User admin interface eth0  
6.70 kbit/s [3 pps] 3.69 kbit/s 2.31 kbit/s  
19:11:27 +0200 | Uptime: 3 days, 21:54:11  
4 Devices 42 Flows

# Allarmi via e-mail

Segnala le anomalie con livelli di *alerts* programmabili

The screenshot displays the ntopng web interface. The main window shows a list of detected alerts under the 'Flow Alerts' tab. The table below summarizes the visible alerts:

Date/Time	Severity	Alert Type	Description
22/08/2019 04:00:12	Warning	! Suspicious Activity	TCP connection refused [Flow: 192.168.1.117 Protocol: TCP]
22/08/2019 12:08:28	Warning	! Suspicious Activity	Suspicious TCP SYN Probing (or server port ...) [L4 Protocol: TCP]
22/08/2019 12:08:28	Warning	! Suspicious Activity	Suspicious TCP SYN Probing (or server port ...) [L4 Protocol: TCP]
22/08/2019 12:08:33	Warning	! Suspicious Activity	Suspicious TCP SYN Probing (or server port ...) [L4 Protocol: TCP]
23/08/2019 15:18:11	Error	! Blacklisted Flow	Client, server or domain is blacklisted [Flow: 1 darkbox.homenet.telecomi...:3000] [L4 Protoc...
23/08/2019 15:18:11	Error	! Blacklisted Flow	Client, server or domain is blacklisted [Flow: 122.228.19.80 @:6745 ⇌ darkbox.homenet.telecomi...:3000] [L4 Protocol: TCP]
23/08/2019 15:18:11	Error	! Blacklisted Flow	Client, server or domain is blacklisted [Flow: 122.228.19.80 @:36271 ⇌ darkbox.homenet.telecomi...:3000] [L4 Protocol: TCP] [Info: 79.26.129.65/ @]
23/08/2019 15:36:56	Error	! Blacklisted Flow	Client, server or domain is blacklisted [Flow: 120.52.152.16 @:58914 ⇌ darkbox.homenet.telecomi...:22] [L4 Protocol: TCP]

An inset window shows the 'Alerts' preferences page, which includes a sidebar menu with categories: Alerts, Alert Endpoints, Protocols, Logging, Network Discovery, and Misc. The main content area lists various alert types with their descriptions and toggle switches:

- SSL Alerts: Toggle alerts generated when the SSL certificate provided by a server does not match the certificate Common Name. (On/Off)
- DNS Alerts: Toggle alerts generated when the DNS query is invalid. (On/Off)
- IP Reassignment Alerts: Toggle alerts generated when an IP address, previously seen with a MAC address, is now seen with another MAC address. This alert might indicate an ARP spoof attempt. (On/Off)
- Remote to Remote Alerts: Toggle alerts generated when the client and the server of a flow are remote. (On/Off)
- Mining Alerts: Toggle alerts generated when traffic from/to hosts known to perform cryptocurrencies mining is detected. (On/Off)
- Malware Alerts: Toggle alerts generated by traffic sent/received by malware-marked hosts. Overnight new blacklist rules are refreshed. (On/Off)
- Device Protocols Alerts: Toggle alerts generated when an anomalous protocol is detected according to the configured device protocols. (On/Off)

# Darkbox® in sintesi...

controlla e previene i cyber-attacchi di nuova generazione

Darkbox, facile da installare e con funzioni modulari:

- PROTEGGE DA VIRUS e MALWARE in maniera completamente diversa da ciò che fanno antivirus o firewall;
- AUMENTA LA SICUREZZA della rete, soddisfacendo i requisiti del GDPR
- SEGNALE COMPORTAMENTI ANOMALI o traffico eccessivo da parte di pc, tablet o smartphone connessi alla rete aziendale
- effettua BACKUP sicuri dei dati più sensibili
- rispetta la PRIVACY, perché controlla il traffico per tipo e protocollo





# Darkbox® in dettaglio...

## Scheda tecnica



Il funzionamento di Darkbox si basa sull'analisi del traffico di rete e sul monitoraggio dei pacchetti, utilizzando la libreria open-source libpcap (C/C++ library for network traffic capture, tcpdump.org).

Il dispositivo, collegato allo switch principale, è in grado di intercettare il traffico, analizzarlo in tempo reale, segnalare o bloccare i comportamenti ritenuti dannosi e tenere un registro (30 gg.) delle informazioni acquisite. Il dispositivo registra le informazioni su due livelli, "warnings", ovvero eventi degni di nota che presentano un qualche livello di rischio e "dangers", eventi ritenuti pericolosi che vengono bloccati (eliminando il pacchetto TCP/IP, se possibile) e segnalati via e-mail.

Il sistema è in grado di rilevare e segnalare i seguenti eventi:

- collegamento di nuovi dispositivi in rete;
- errori nelle richieste al DNS;
- errori nei certificati HTTPS;
- flussi "remoto su remoto", quando la rete controllata ospita traffico dall'esterno verso l'esterno;
- attività di mining di bitcoin effettuata da dispositivi della rete monitorata;
- flussi di grandi dimensioni in download e upload;
- prevenzione di malware, sulla base del traffico indirizzato a particolari indirizzi IP presenti in blacklist aggiornata quotidianamente;

Darkbox è in grado anche di riconoscere il traffico generato dall'attività di oltre 250 applicativi molto diffusi (L7 protocol), come chat (WhatsApp, WeChat, Telegram, ecc.), cloud (Dropbox, BitTorrent), streaming (YouTube, Netflix ecc.). Per tale traffico possono essere impostati allarmi di vario livello. Oltre che come sistema di prevenzione, Darkbox registra tutte le attività di rete, che possono essere utilmente consultate in fase di *incident response*.

Per funzionare è richiesto il collegamento ethernet verso il gateway della rete da monitorare. L'installazione ottimale prevede il collegamento a switch dotati di port replication. La gestione è centralizzata, Darkbox si collega periodicamente al server attraverso VPN, per comunicare il suo stato (acceso, aggiornato, ecc.). Da remoto sono possibili sia la gestione che il monitoraggio.

# Dicono di noi...

Il Sole 24 Ore, 12 marzo 2019

SICUREZZA INFORMATICA > REALTA' ECCELLENTI

20

Martedì 12 Marzo 2019 Il Sole 24 Ore

## Speciale SICUREZZA INFORMATICA - Realtà Eccellenti

### I vostri dati sono al sicuro?

Il recente boom del CYBER CRIME rende la sicurezza informatica una responsabilità dell'intera organizzazione e non solo un ruolo dell'IT manager. I dati della vostra azienda sono veramente al sicuro? Le protezioni perimetrali (firewall, IDS), antivirus e politiche restrittive di accesso vi proteggono da com-

portamenti incauti di dipendenti o clienti? La CYBER SECURITY richiede un nuovo approccio, mediante l'identificazione degli ostacoli, l'attenzione ai rischi futuri e la necessità di lavorare con un unico partner per la sicurezza. Darkbox si occupa dal 2002 di Digital Forensic, offre consulenza a Forze dell'Ordine e

Autorità Giudiziaria in materia di prevenzione e investigazione di crimini informatici e fornisce soluzioni per network & mobile security. L'azienda è specializzata nel penetration testing per l'individuazione di falle di sicurezza nella rete aziendale e nei dispositivi mobili. Scopri tutti i nostri servizi su [www.darkbox.it](http://www.darkbox.it)



Il Sole 24 Ore, 10 marzo 2020

OBIETTIVO SICUREZZA: tecnologie, intelligence e cybersecurity

Il Sole 24 Ore Martedì 10 Marzo 2020

25

## Speciale OBIETTIVO SICUREZZA: TECNOLOGIE, INTELLIGENCE E CYBERSECURITY - Realtà Eccellenti

### Darkbox contro i rischi cyber

I dispositivi tradizionali come Firewall e Antivirus non sono più sufficienti per una protezione adeguata della rete aziendale. Darkbox, pensato per gli attacchi di nuova generazione, aumenta la sicurezza in linea con quanto disposto dal GDPR in

materia di tutela dei dati. Cos'è Darkbox? Un piccolo dispositivo che, collegato allo switch principale, monitora la rete analizzando i pacchetti e il tipo di traffico, traccia i dispositivi e segnala i comportamenti anomali tramite e-mail. Ma il rischio Cyber

non è eliminabile al 100%. Se succede un danno? Darkbox non è solo hardware ma un sistema integrato di servizi. Da quest'anno Darkbox si avvale della collaborazione con distributori di polizze cyber risk che riconoscono uno sconto sul pre-

mio. In questo modo si completa l'intero perimetro del rischio cyber con l'aumento della sicurezza e il risarcimento in caso di danno, compresi i costi per l'assistenza e il ripristino della rete. [www.darkbox.it](http://www.darkbox.it)

