uania
SHIELD

Il servizio di sicurezza
informatica completo
e **Plug & Play.**

uania
ALWAYS CONNECTED

uania.com

Cybersecurity, i rischi per le aziende

Le aziende oggi sono sempre più interconnesse tra loro e internet è sempre più un mezzo per generare business.
Proprio per questo, Uania è nata ed ha operato con l'obiettivo di offrire alle aziende italiane una soluzione che rendesse le connettività più veloci e stabili, anche in quelle aree scoperte dalla banda larga.
Il tema della performance della connettività si lega strettamente a quello della sicurezza della navigazione, che spesso espone le PMI a vulnerabilità che limitano lo sviluppo delle aziende.

Il CLUSIT ha stimato che nel 2021 circa la metà delle minacce alla cybersecurity in Italia ha avuto un impatto "critico" (13%) e "alto" (36%) (*). La severità della situazione è confermata anche dai dati globali, che dimostrano un aumento di oltre il 50% degli attacchi informatici settimanali subiti dalle aziende rispetto al 2020. Tra i settori maggiormente colpiti quello dell'istruzione e della ricerca (+75%), mentre il 13% degli attacchi totali del 2021 in Italia hanno riguardato il ramo del finance (8%) e quello della sanità (5%).
Anche i Cloud Services Provider sono stati esposti a pericoli che hanno limitato e spesso impedito la raggiungibilità di servizi strategici per le imprese. Il crescente utilizzo di dispositivi privati sui luoghi di lavoro e per motivi produttivi, oltre alla crescente digitalizzazione dei luoghi di produzione anche con macchinari sempre più interattivi grazie alla IoT, ha visto estendersi notevolmente la superficie vulnerabile ai cyberattacchi.
È stato stimato che nel 2021, almeno un dipendente del 46% delle aziende ha scaricato un malware tramite dispositivo mobile, che ha poi minacciato la salute della rete e dei dati.

(*) https://www.mmn.it/wp-content/uploads/2021/05/Rapporto-Clusit_03-2021-web.pdf

Per dare una risposta a queste esigenze, Uania ha sviluppato il servizio UaniaShield, un livello di protezione completo, semplice e scalabile, che permette alle PMI di non dover sostenere i costi e le complessità di implementazione fisica di una soluzione di fascia enterprise.

I vantaggi di Uania SHIELD

Implementazione classica

Alto costo di implementazione

I firewall vengono spesso venduti con un costo di start up per l'acquisto dell'hardware + licenza annuale/biennale per servizi anche granulari.

Difficile configurazione

È spesso difficile configurare in maniera efficiente e performante i servizi di protezione per ottenere risultati che evitino "falsi positivi"

Difficile scalabilità

Le soluzioni implementate con hardware fisico installate presso il cliente sono spesso un limite alla crescita dello stesso e del volume di traffico da proteggere, costringendo ad un cambio di dispositivo "in corso d'opera" che può provocare continui investimenti e downtime.

Reportistica complessa

Le reportistiche generate dai firewall sono spesso troppo tecniche, specifiche e dettagliate, utili per un tecnico ma inutili al cliente finale che non percepisce, nel concreto, l'operato del firewall e la sua effettiva utilità.

Servizio Uania Shield

Basso costo di implementazione

La soluzione ha un unico canone mensile che racchiude tutti i servizi di protezione senza nessun altro costo aggiuntivo.

Configurazione plug&play

La soluzione è preconfigurata da esperti con le massime certificazioni sulle specifiche piattaforme e può essere personalizzata.

Massima scalabilità

Il database sempre aggiornato per fronteggiare ogni nuova minaccia informatica rende la estremamente scalabile e pronta ad adattarsi in qualsiasi momento a tutte le necessità, tutto senza dover fare alcun investimento in hardware specifico.

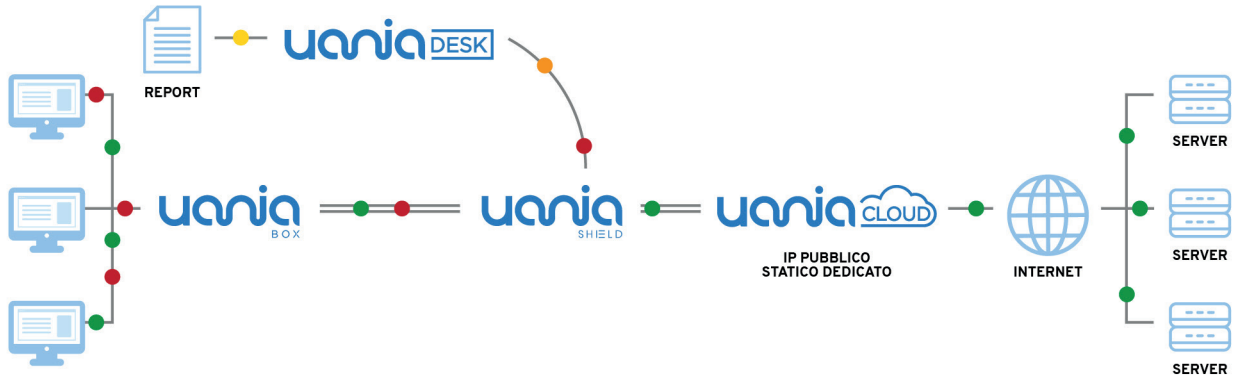
Reportistica agile

La piattaforma di gestione, oltre ad una dashboard live che racchiude tutti i parametri operativi del firewall, genera un report mensile di poche pagine che illustra l'operato del servizio e la sua effettiva utilità alla protezione attiva dell'azienda.

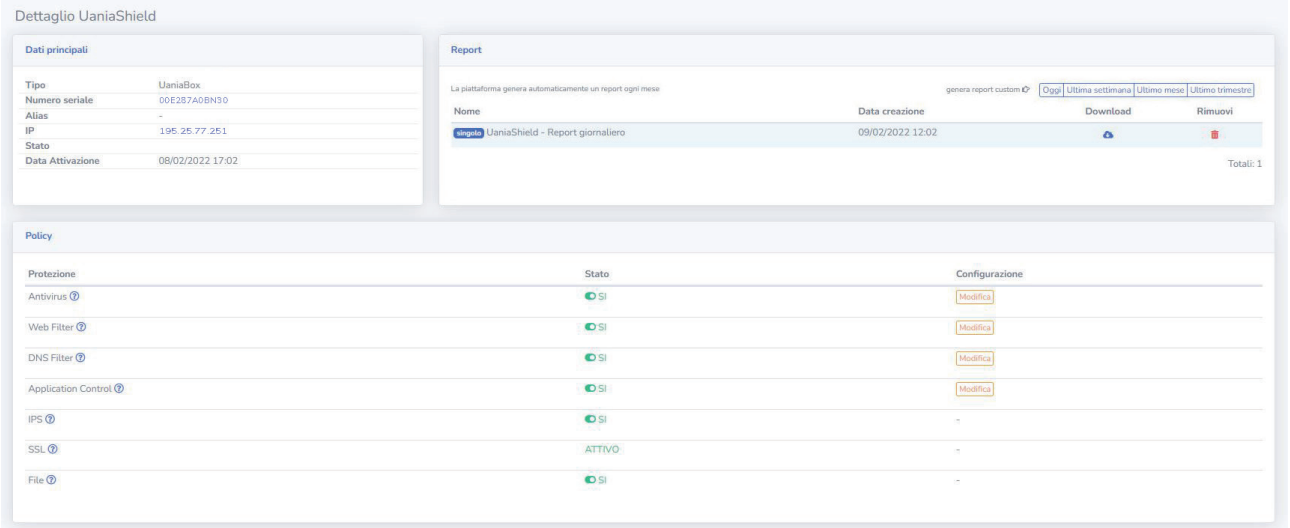
Come funziona Uania Shield

UaniaShield è un servizio di protezione UTM perimetrale IaaS (Infrastructure as a Service) che consente di proteggere il traffico internet dell'azienda senza dover installare un firewall nella rete.
La protezione avviene nel nostro cloud utilizzando apparati dotati delle massime licenze disponibili sul mercato, per garantire al cliente protezione senza alcun compromesso.
Il traffico filtrato viene consegnato direttamente sull'IP pubbico statico e dedicato della soluzione Uania.
UaniaShield è stato progettato per consentire una installazione e gestione semplice, rapida e totalmente Plug&Play, garantendo le massime performance possibili in tema sicurezza, affidando la protezione ad uno dei top vendor presenti sul mercato secondo Gartner® (*).

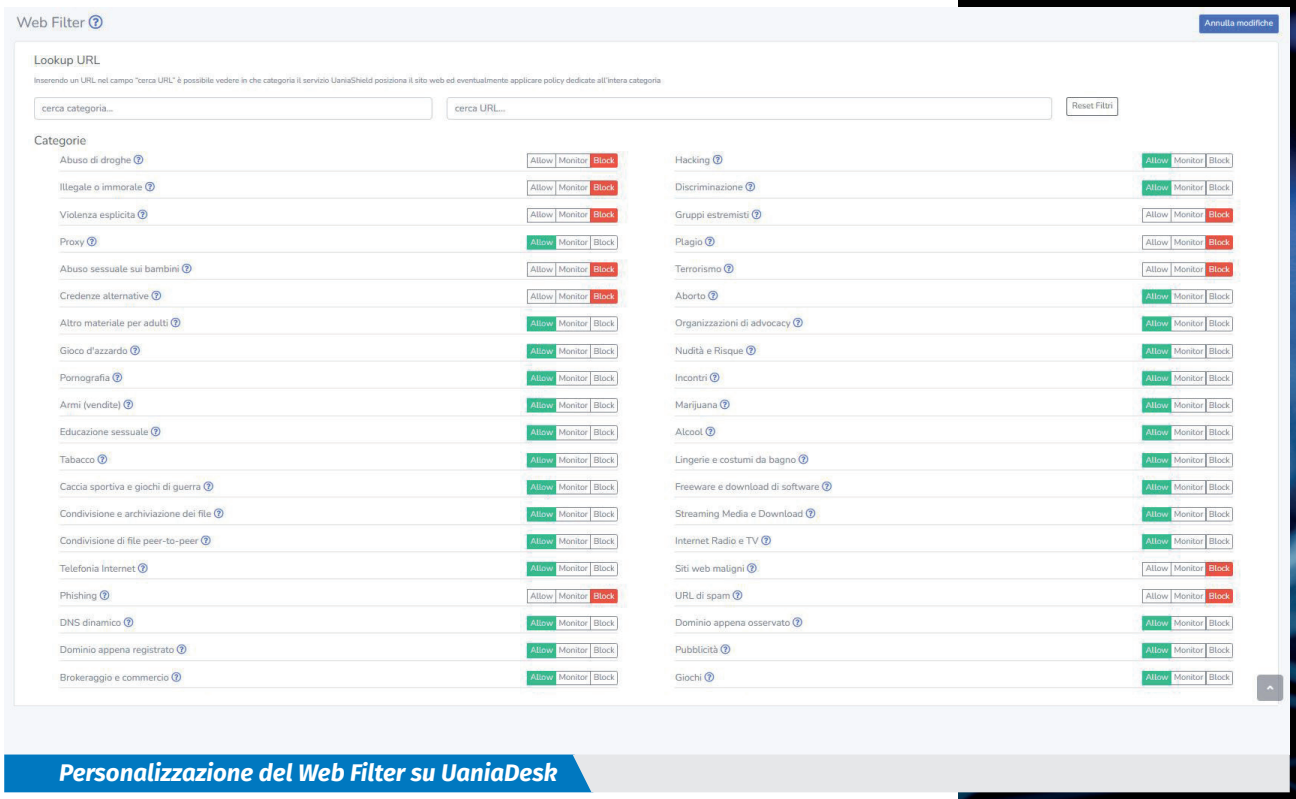
(*) https://www.fortinet.com/solutions/gartner-network-firewalls



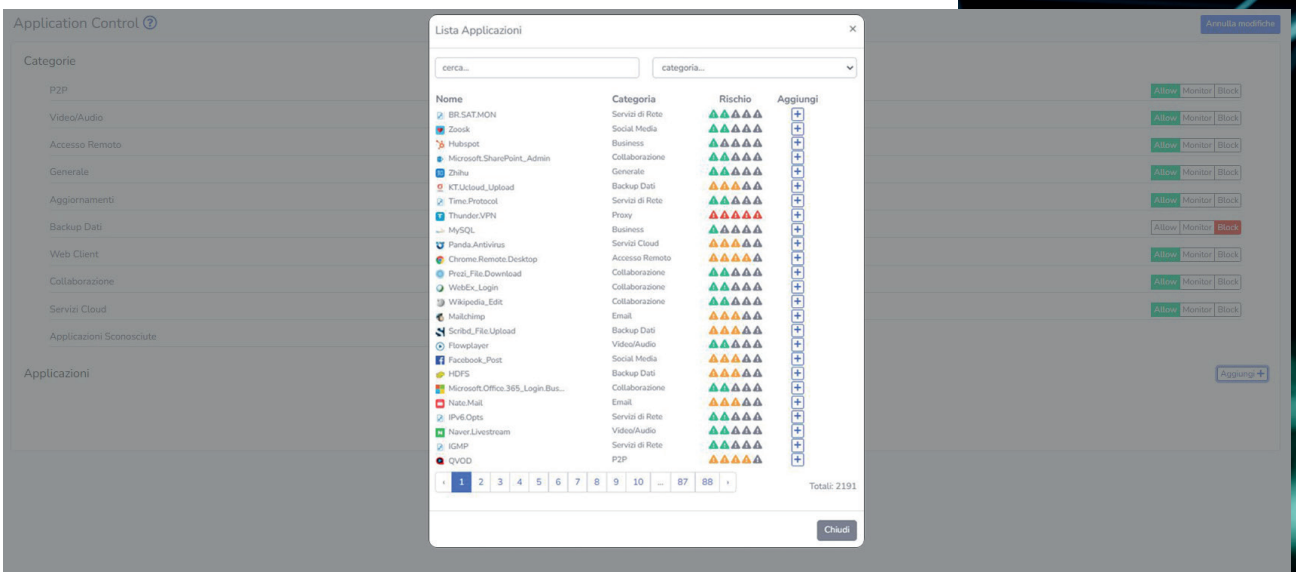
Infrastruttura del servizio



Pagina di dettaglio su UaniaDesk



Personalizzazione del Web Filter su UaniaDesk



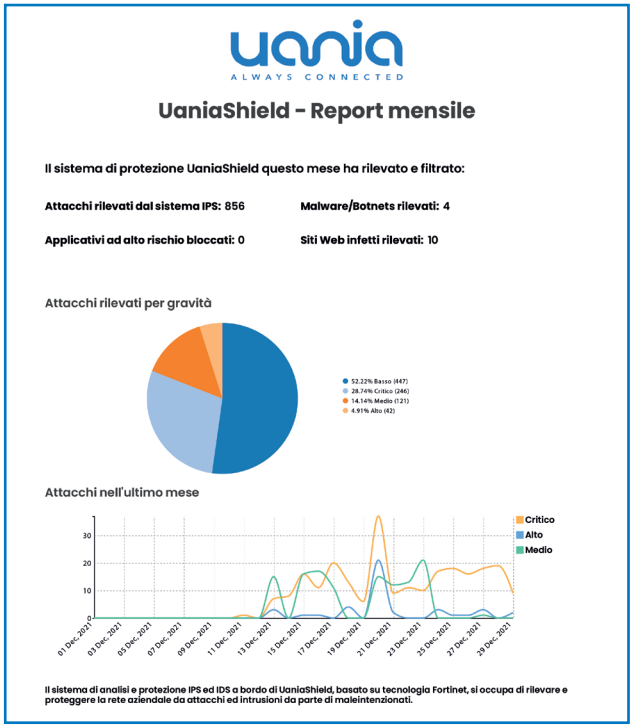
Personalizzazione dell'Application Control

UaniaShield permette di attivare e personalizzare:

ANTIVIRUS	Il servizio AntiVirus integrato in UaniaShield si occupa di analizzare il traffico, da e verso UaniaCloud, alla ricerca di potenziali virus, spyware e altre minacce. Una volta trovato, il virus viene bloccato e viene segnalata l'azione nel report mensile presente in piattaforma.
WEB FILTER	Il servizio di Web Filter integrato in UaniaShield fornisce una protezione completa dalle minacce, tra cui ransomware, furto di credenziali, phishing e altri attacchi via web. Utilizza l'analisi e la correlazione del comportamento basate sull'intelligenza artificiale per bloccare quasi immediatamente gli URL dannosi sconosciuti, con falsi negativi quasi pari a zero. Il servizio permette inoltre di decidere quali categorie sono permesse o meno e, in caso di necessità, di monitorarle (il traffico viene accettato e monitorato nel report mensile).
DNS FILTER	Il servizio di DNS Filter integrato in UaniaShield fornisce una protezione completa da minacce come botnet, phishing, ecc. bloccando domini con bassa reputazione o malevoli. Il servizio permette inoltre di decidere quali categorie sono permesse o meno e, in caso di necessità, di monitorarle (il traffico viene accettato e monitorato nel report mensile).
APPLICATION CONTROL	Il servizio di Application Control integrato in UaniaShield permette di limitare o monitorare l'accesso a categorie o specifiche applicazioni in maniera semplice e agevole.
IPS	Il servizio di protezione IPS integrato in UaniaShield è il servizio che previene le intrusioni non autorizzate ai sistemi aziendali. Il sistema include diverse opzioni di motori di ispezione, feed di threat intelligence e protezione da minacce avanzate per difendersi da queste minacce sconosciute. Il sistema protegge da attacchi mirati avanzati e zero-day, ransomware e malware polimorfici.
SSL	Il servizio di ispezione SSL integrato in UaniaShield si occupa di analizzare ed assicurarsi che tutti i certificati SSL utilizzati durante la navigazione siano autentici e sicuri.
FILE INSPECTION	Il servizio di protezione FILE integrato in UaniaShield analizza i file trasmessi da e verso UaniaCloud bloccando quelli malevoli, raggiunge questo risultato grazie al connubio con una SandBox dedicata.

Reportistica

UaniaShield consente di generare un documento che sintetizza in modo completo e leggibile l'attività svolta dal servizio di protezione.
La reportistica di UaniaShield mette a disposizione di dealer e utente finale un PDF agile da consultare con il riepilogo degli attacchi rilevati e bloccati, delle vulnerabilità riscontrate e protette, dei malware, botnets e spyware riconosciuti oltre al dettaglio dei siti bloccati.



uania
ALWAYS CONNECTED

UaniaShield - Report mensile

Il sistema di protezione UaniaShield questo mese ha rilevato e filtrato:

Attacchi rilevati dal sistema IPS: 856 **Malware/Botnets rilevati: 4**

Applicativi ad alto rischio bloccati: 0 **Siti Web infetti rilevati: 10**

Attacchi rilevati per gravità

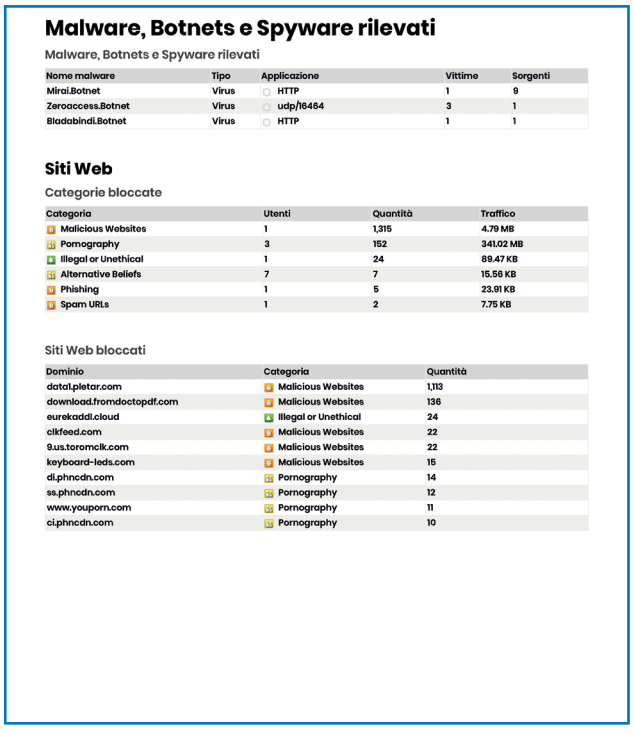
Attacchi nell'ultimo mese

Il sistema di analisi e protezione IPS ed IDS a bordo di UaniaShield, basato su tecnologia Fortinet, si occupa di rilevare e proteggere la rete aziendale da attacchi ed intrusioni da parte di malintenzionati.

Vulnerabilità riscontrate

Vulnerabilità riscontrate

Criticità	Nome vulnerabilità	Tipo	CVE-ID	Vittime	Numero attacchi
5	Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	Improper Authentication		2	66
5	Apache.Log4j.Error.Log.Remote.Code.Execution	Permission/Priviledge/Access Control	CVE-2021-44228,CVE-2021-45046	1	60
5	Apache.Log4j.Error.Log.Remote.Code.Execution	Permission/Priviledge/Access Control	CVE-2021-4104,CVE-2021-44228,CVE-2021-45046	1	31
5	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	OS Command Injection	CVE-2015-2051,CVE-2019-10891	1	28
5	Apache.Log4j.Error.Log.Remote.Code.Execution	Permission/Priviledge/Access Control	CVE-2021-44228	1	15
5	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Code Injection		1	13
5	Dasan.GPON.Remote.Code.Execution	OS Command Injection	CVE-2018-10561,CVE-2018-10562	1	12
5	Zeroaccess.Botnet			3	6
5	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Code Injection	CVE-2019-9082,CVE-2018-20082	1	4
5	Wireshark.ENTTEC.DMX.Data.RLE.Buffer.Overflow	Buffer Errors	CVE-2010-4538	2	4
5	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	Improper Authentication	CVE-2017-11317,CVE-2017-11357,CVE-2019-18935	1	2
5	Bladabindi.Botnet			1	2
5	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Code Injection	CVE-2017-9841	1	2
5	Gh0st.Rat.Botnet			1	1
4	malicious-url			1	18
4	Mirai.Botnet			1	9
4	Linux.Kernel.TCP.SACK.Panic.DoS	DoS	CVE-2019-11477,CVE-2019-11478,CVE-2019-11479	2	8
4	Axis.SSI.camnbr.Remote.Command.Execution	Code Injection		1	3
4	VACRON.CCTV.Board.CGI.cmd.Parameter.Command.Execution	OS Command Injection		1	2



Malware, Botnets e Spyware rilevati

Malware, Botnets e Spyware rilevati

Nome malware	Tipo	Applicazione	Vittime	Sorgenti
Mirai.Botnet	Virus	HTTP	1	9
Zeroaccess.Botnet	Virus	udp/16464	3	1
Bladabindi.Botnet	Virus	HTTP	1	1

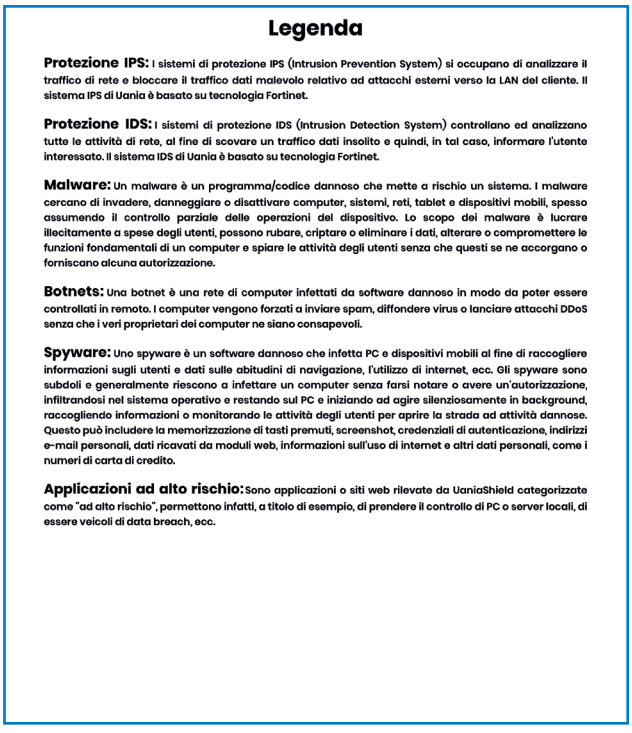
Siti Web

Categorie bloccate

Categoria	Utenti	Quantità	Traffico
Malicious Websites	1	1,315	4.79 MB
Pornography	3	152	341.02 MB
Illegal or Unethical	1	24	89.47 KB
Alternative Beliefs	7	7	15.56 KB
Phishing	1	5	23.91 KB
Spam URLs	1	2	7.75 KB

Siti Web bloccati

Dominio	Categoria	Quantità
data1.pletar.com	Malicious Websites	1,113
download.fromdoctopdf.com	Malicious Websites	136
eurekaddl.cloud	Illegal or Unethical	24
clkfeed.com	Malicious Websites	22
9.us.toromclk.com	Malicious Websites	22
keyboard-leds.com	Malicious Websites	15
dl.phncdn.com	Pornography	14
ss.phncdn.com	Pornography	12
www.youporn.com	Pornography	11
cl.phncdn.com	Pornography	10



Legenda

Protezione IPS: I sistemi di protezione IPS (Intrusion Prevention System) si occupano di analizzare il traffico di rete e bloccare il traffico dati malevolo relativo ad attacchi esterni verso la LAN del cliente. Il sistema IPS di Uania è basato su tecnologia Fortinet.

Protezione IDS: I sistemi di protezione IDS (Intrusion Detection System) controllano ed analizzano tutte le attività di rete, al fine di scovare un traffico dati insolito e quindi, in tal caso, informare l'utente interessato. Il sistema IDS di Uania è basato su tecnologia Fortinet.

Malware: Un malware è un programma/codice dannoso che mette a rischio un sistema. I malware cercano di invadere, danneggiare o disattivare computer, sistemi, reti, tablet e dispositivi mobili, spesso assumendo il controllo parziale delle operazioni del dispositivo. Lo scopo dei malware è lucrare illecitamente a spese degli utenti, possono rubare, criptare o eliminare i dati, alterare o compromettere le funzioni fondamentali di un computer e spiare le attività degli utenti senza che questi se ne accorgano o forniscano alcuna autorizzazione.

Botnets: Una botnet è una rete di computer infettati da software dannoso in modo da poter essere controllati in remoto. I computer vengono forzati a inviare spam, diffondere virus o lanciare attacchi DDoS senza che i veri proprietari dei computer ne siano consapevoli.

Spyware: Uno spyware è un software dannoso che infetta PC e dispositivi mobili al fine di raccogliere informazioni sugli utenti e dati sulle abitudini di navigazione, l'utilizzo di internet, ecc. Gli spyware sono subdoli e generalmente riescono a infettare un computer senza farsi notare o avere un'autorizzazione, infiltrandosi nel sistema operativo e restando sul PC e iniziando ad agire silenziosamente in background, raccogliendo informazioni o monitorando le attività degli utenti per aprire la strada ad attività dannose. Questo può includere la memorizzazione di tasti premuti, screenshot, credenziali di autenticazione, indirizzi e-mail personali, dati ricavati da moduli web, informazioni sull'uso di internet e altri dati personali, come i numeri di carta di credito.

Applicazioni ad alto rischio: Sono applicazioni o siti web rilevate da UaniaShield categorizzate come "ad alto rischio", permettono infatti, a titolo di esempio, di prendere il controllo di PC o server locali, di essere veicoli di data breach, ecc.

ALWAYS CONNECTED

uania.com

info@uania.com
T: +39 080 222 35 74

SOCIAL

https://www.uania.com/
https://www.facebook.com/uaniaitalia
https://www.instagram.com/uania_italia/
https://www.linkedin.com/company/uania/

Copyright © 2022 Uania - All Rights Reserved