WORKSHOP GARR 2020
NET MAKERS

Effetto Covid-19: gli effetti del lockdown sulla sicurezza informatica

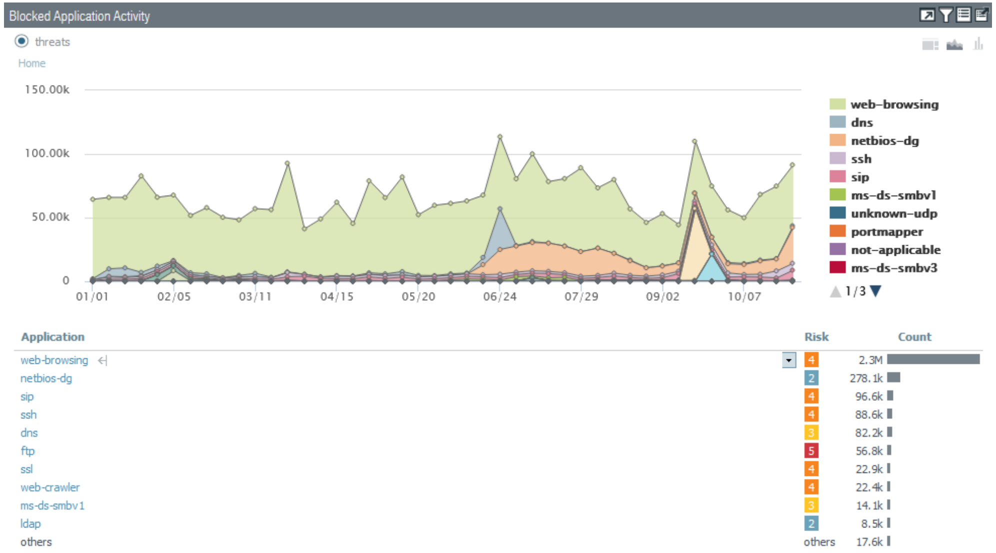
Andrea Sartori

UNIVERSITÀ
di VERONA

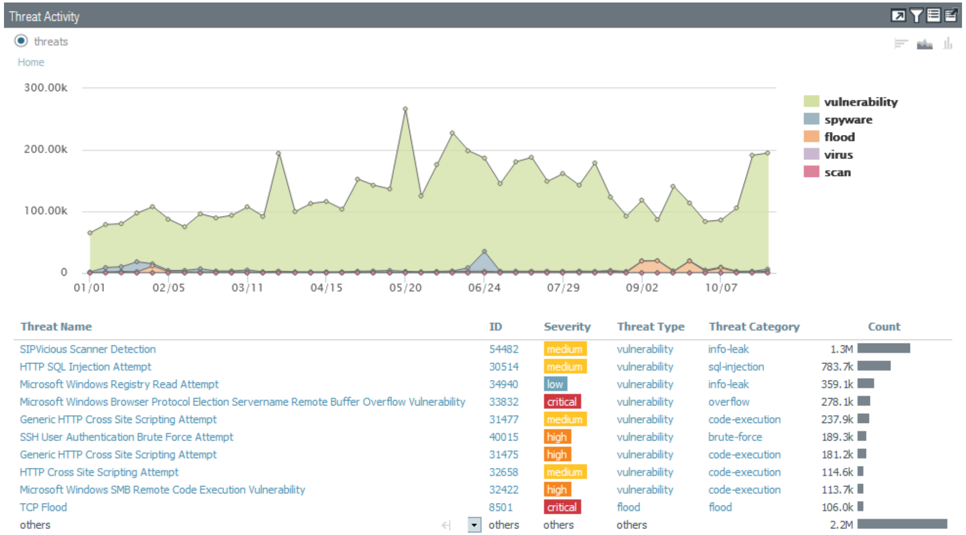
Direzione
SISTEMI INFORMATIVI
E TECNOLOGIE

Covid-19 @UniVR

Trend Applicazioni bloccate


Blocked Application Activity
threats
Home
150.00k
100.00k
50.00k
0
01/01
02/05
03/11
04/15
05/20
06/24
07/29
09/02
10/07
web-browsing
dns
netbios-dg
ssh
sip
ms-ds-smbv1
unknown-udp
portmapper
not-applicable
ms-ds-smbv3
1/3

Application	Risk	Count
web-browsing	4	2.3M
netbios-dg	2	278.1k
sip	4	96.6k
ssh	4	88.6k
dns	3	82.2k
ftp	5	56.8k
ssl	4	22.9k
web-crawler	4	22.4k
ms-ds-smbv1	3	14.1k
ldap	2	8.5k
others	others	17.6k


Threat Activity
threats
Home
300.00k
200.00k
100.00k
0
01/01
02/05
03/11
04/15
05/20
06/24
07/29
09/02
10/07
vulnerability
spyware
flood
virus
scan

Threat Name	ID	Severity	Threat Type	Threat Category	Count
SIPVicious Scanner Detection	54482	medium	vulnerability	info-leak	1.3M
HTTP SQL Injection Attempt	30514	medium	vulnerability	sql-injection	783.7k
Microsoft Windows Registry Read Attempt	34940	low	vulnerability	info-leak	359.1k
Microsoft Windows Browser Protocol Election Servername Remote Buffer Overflow Vulnerability	33832	critical	vulnerability	overflow	278.1k
Generic HTTP Cross Site Scripting Attempt	31477	medium	vulnerability	code-execution	237.9k
SSH User Authentication Brute Force Attempt	40015	high	vulnerability	brute-force	189.3k
Generic HTTP Cross Site Scripting Attempt	31475	high	vulnerability	code-execution	181.2k
HTTP Cross Site Scripting Attempt	32658	medium	vulnerability	code-execution	114.6k
Microsoft Windows SMB Remote Code Execution Vulnerability	32422	high	vulnerability	code-execution	113.7k
TCP Flood	8501	critical	flood	flood	106.0k
others	others	others	others		2.2M

Trend minacce rilevate