



Banche e Sicurezza 26 Maggio 2021

Gli Attacchi alla supply chain: dal man in the middle alla backdoor.

IL Gruppo TinextaCyber

Opera attraverso le tre società
Corvallis, Yoroi e Swascan.

- HUB Italiano della cybersecurity,
- Focus sui temi della sicurezza digitale,
- Servizi basati su asset proprietari
- Convergenza tra Digital Trust e Cybersecurity,
- Mission e Shareholder Istituzionali



80 M€

VOLUME
AFFARI

900

DIPENDENTI

Pierguido Iezzi

Cyber Security Director e co-founder di Swascan con oltre 30 anni di esperienza nel mondo della Cyber Security. Laureato in Scienze dell'informazione, ha avuto la fortuna di operare a livello nazionale e internazionale in grandi contesti aziendali e nelle più grandi multinazionali come referente Cyber Security. Autore di diverse pubblicazioni, collabora regolarmente come Autore e Contributor a una serie di testate giornalistiche tra cui la colonna "Hacker News" de Il Foglio. Keynote speaker e testimonial presso università, eventi nazionali e internazionali.

p.iezzi@swascan.com

swascan.com



Cos'è Swascan ?



La prima suite interamente in **Cloud** e **OnPremise** che permette di:

IDENTIFICARE



ANALIZZARE



RISOLVERE



Identifica, analizza e risolve le **criticità, problematiche e vulnerabilità** di Sicurezza Informatica degli asset Aziendali a livello di:

Siti Web

Applicazioni web

Mobile App

Network

Cyber
Research
Team:
**Vulnerability
Disclosure**



[Scopri di più](#)

Lenovo

[Scopri di più](#)

NOKIA

[Scopri di più](#)



[Scopri di più](#)



[Scopri di più](#)



[Scopri di più](#)



[Scopri di più](#)



[Scopri di più](#)

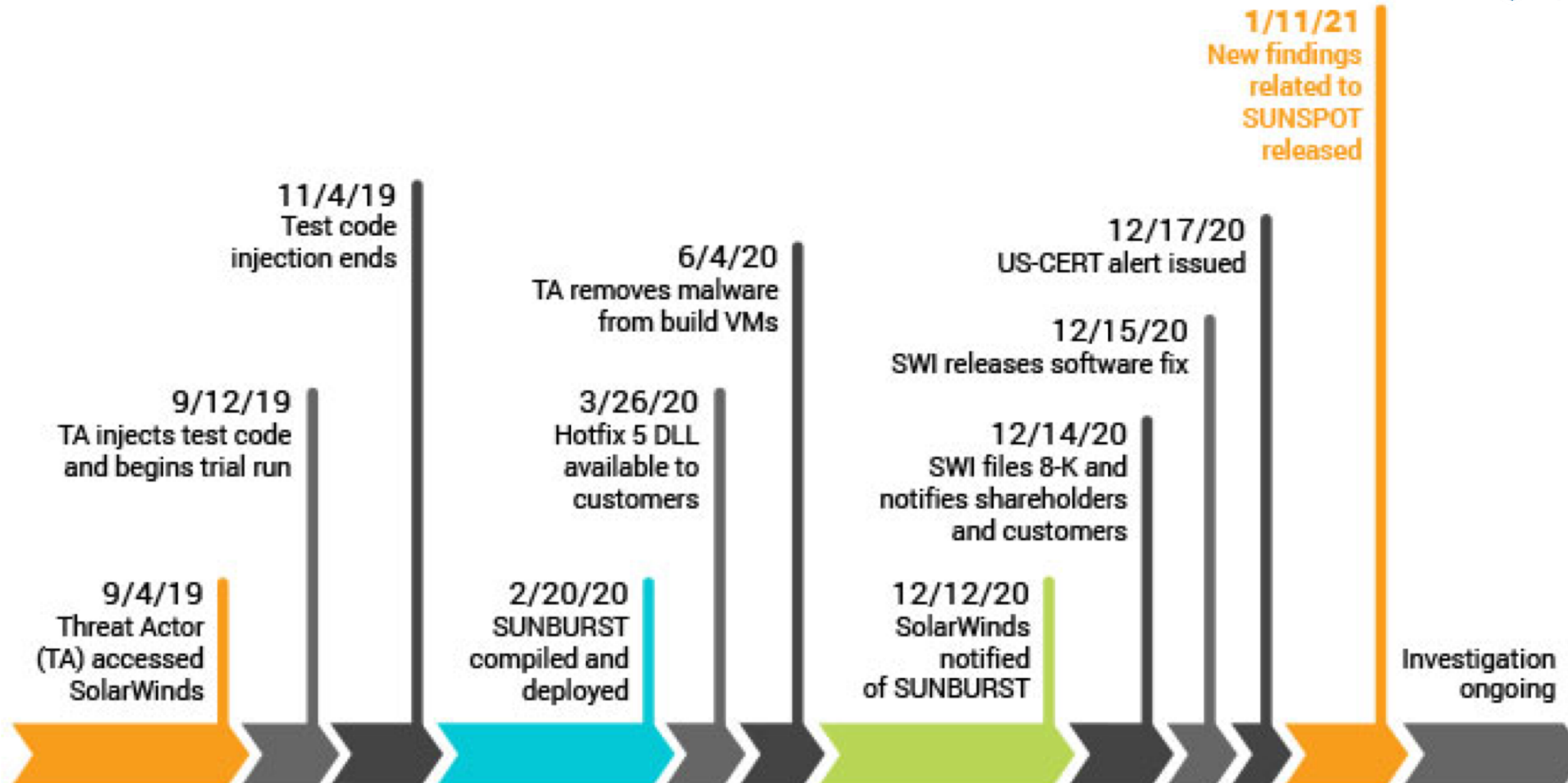


[Scopri di più](#)



[Scopri di più](#)

Attack Timeline - Overview



All events, dates, and times approximate and subject to change; pending completed investigation.

1

2



Vinoth Kumar @vinodsparrow · 14 dic 2020

Was reading about a sophisticated attack on FireEye leveraging Solarwinds. Hmmm how that would happened? 🤔. Then realized their password was *****123 🔄 #FireEye #SolarWinds

Open Github Repo Leaking FTP Credentials of <http://downloads.solarwinds.com>



Vinoth Kumar
Tue 2019-11-19 14:32
To: psirt@solarwinds.com

Hi Team,

I have found a public Github repo which is leaking ftp credential belongs to SolarWinds.

Repo URL: <https://github.com/>

[.config](#)

Downloads Url: <http://downloads.solarwinds.com>

FTP Url: <ftp://solarwinds.upload.akamai.com>

Username:

Password:

POC: <http://downloads.solarwinds.com/test.txt>

I was able to upload a test POC.

Via this any hacker could upload malicious exe and update it with release SolarWinds product.

[illegible]

52

↕ 917

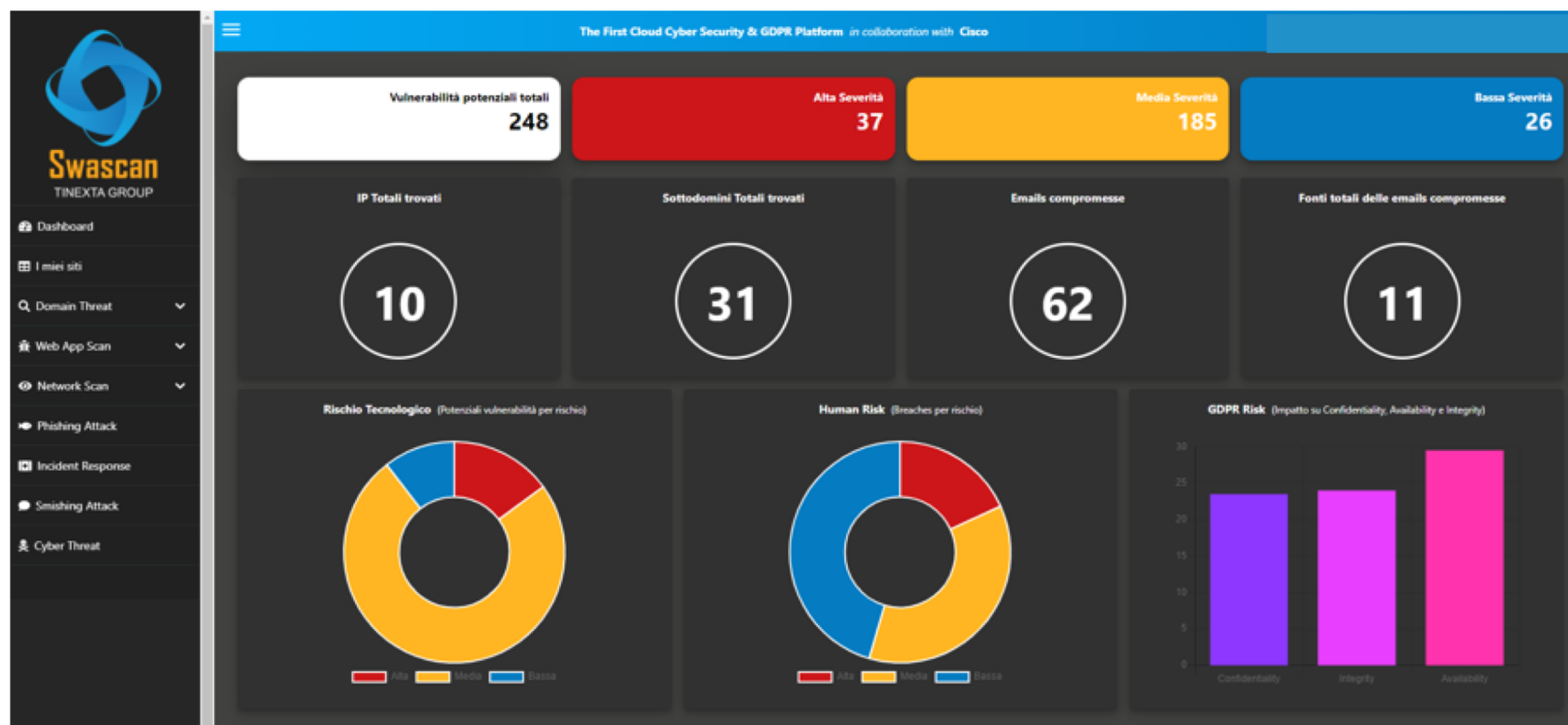
2.116



Domain Threat Intelligence



1



© 2014 Pearson Education, Inc.



These Data Represent the Active computers infected with Botnets which have been engaged with Target.inset.ch We Provide all the data related to Botnet which can be Employees, Customers or your Partners which they access the domain inset.ch A botnet is a network of computer infected with malware, spyware, key loggers, etc. The "bot hardener" (the botnet manager) can use its botnet network to launch attacks (e.g. DDoS), or instruct it to steal credentials (e-banking, corporate intranet, civil and criminal legal liability, information theft, industrial espionage, etc.)

```
host: http://www.a[REDACTED]
user: [REDACTED]
pass: [REDACTED]
```


Perché Parliamo di Supply Chain Risk Indicators?



Perchè Gestire la Supply Chain Risk?




Compliance



Standard/Best
Practise



Cyber
Protection



Cyber
Management

Supplier Chain Cyber&Risk

Uno strumento finalizzato alla verifica dei rischi connessi alla gestione del portafoglio fornitori. Tiene conto della dimensione del rischio di continuità di fornitura e del rischio cyber del fornitore.

Il servizio permette di identificare e individua le informazioni pubbliche e semipubbliche le vulnerabilità disponibili pubblicamente relative al dominio ed email compromesse del fornitore

Il servizio ha lo scopo e l'obiettivo di individuare le eventuali informazioni pubbliche disponibili a livello OSINT e CLOSINT relative ad un determinato target. L'attività viene effettuata attraverso un processo di ricerca, individuazione e selezione delle informazioni disponibili pubblicamente relative al dominio di interesse.

Supplier Cyber Risk Indicator

- Numero delle Vulnerabilità
- Numero Email compromesse
- Rischio Tecnologico
- Rischio Umano
- Rischio GDPR

Servizio:

- Servizio svolto dal personale Swascan
- Report su base mensile



Output: Fornitori analizzati



Fornitori/Responsabili	TOTALE VULNERABILITA'	HIGH	MEDIUM	LOW	EMAIL COMPROMISED	GDPR IMPACT CONFIDENTIALITY	GDPR IMPACT INTEGRITY	GDPR IMPACT AVAILABILITY
XXXXXXX	64	3	55	6	110	26	26	41
XXXXXXX	0	0	0	0	37	0	0	0
XXXXXXX	0	0	0	0	35	0	0	0
XXXXXXX	2	0	2	0	2	1	1	0
XXXXXXX	46	10	33	3	187	24	24	41
XXXXXXX	0	0	0	0	0	0	0	0
XXXXXXX	74	15	46	13	981	43	43	49
XXXXXXX	7	4	2	1	80	8	8	9
XXXXXXX	0	0	0	0	55	0	0	0
XXXXXXX	0	0	0	0	151	0	0	0

Output: Cyber Risk Indicators Marzo 2021



Potential Technology Risk

19,3

Average Potential
Vulnerabilities

High Severity
3,2%

Medium Severity
13,8%

Low Severity
2,3%

Potential GDPR Risk

Confidentiality

10,1%

Integrity

10,2%

Availability

14%

Potential Human Risk

1638

Total
Compromised
Email

163,8

Average
Compromised
Email

Output: Technology Risk



Average
Potential
Vulnerabilities

50



+3%

Percentuale di High rispetto
al mese precedente.

High Severity
33%



+3%

% rispetto
al mese precedente.

Medium Severity
33%



ND

% rispetto
al mese precedente.

Low Severity
33%



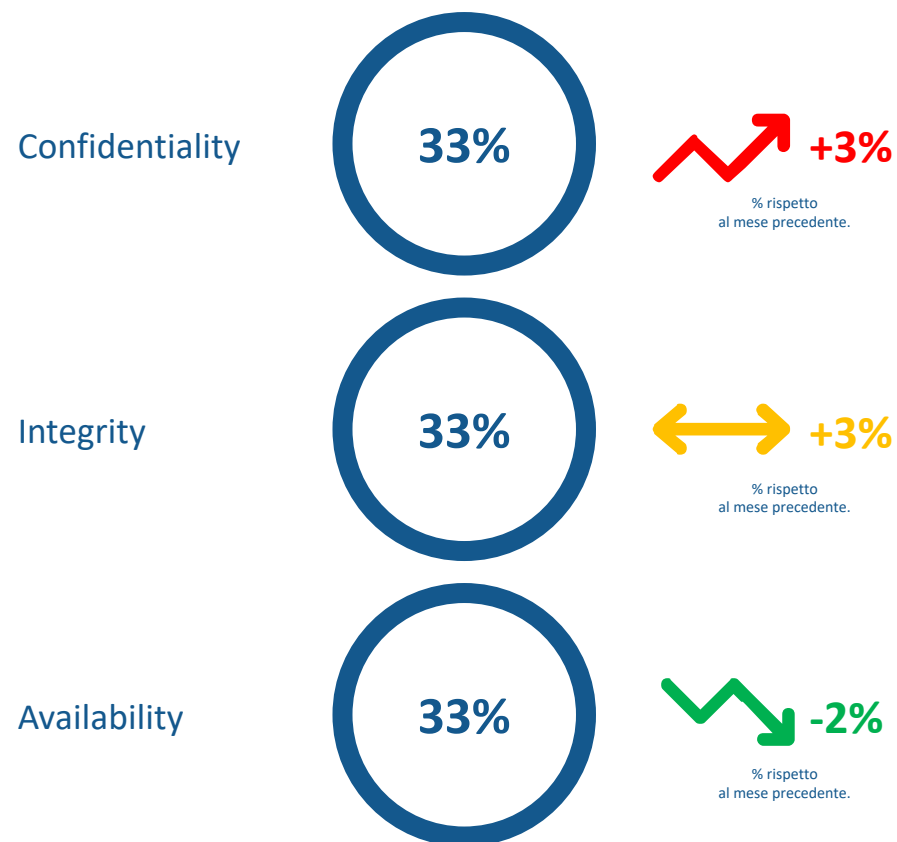
-2%

% rispetto
al mese precedente.

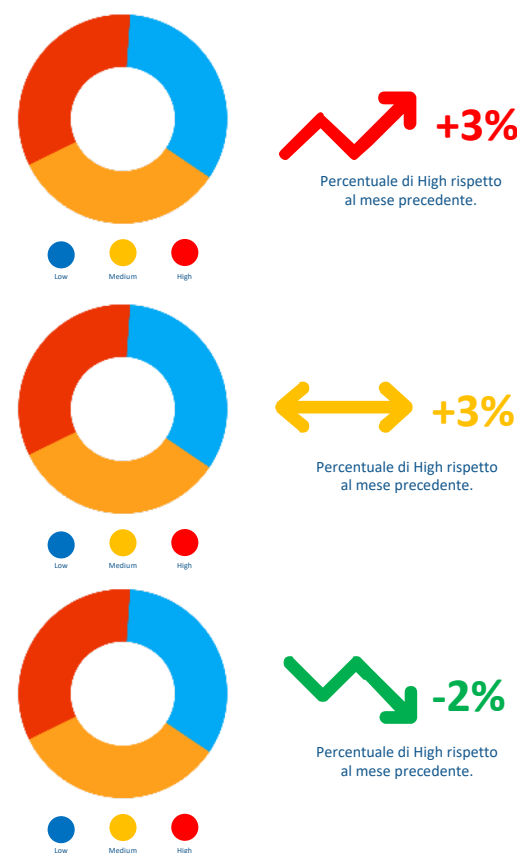
Output: Compliance Risk



Average GDPR Vulnerability Impact



Average GDPR Risk



Output: Social Engineering Risk



Total Compromised Email



200

From **15** different sources



10

Average compromised email for (sector) companies



Grazie



p.iezzi@swascan.com

swascan.com



TINEXTA
CYBER

Banche e Sicurezza 26 Maggio 2021

Gli Attacchi alla supply chain: dal man in the middle alla backdoor.