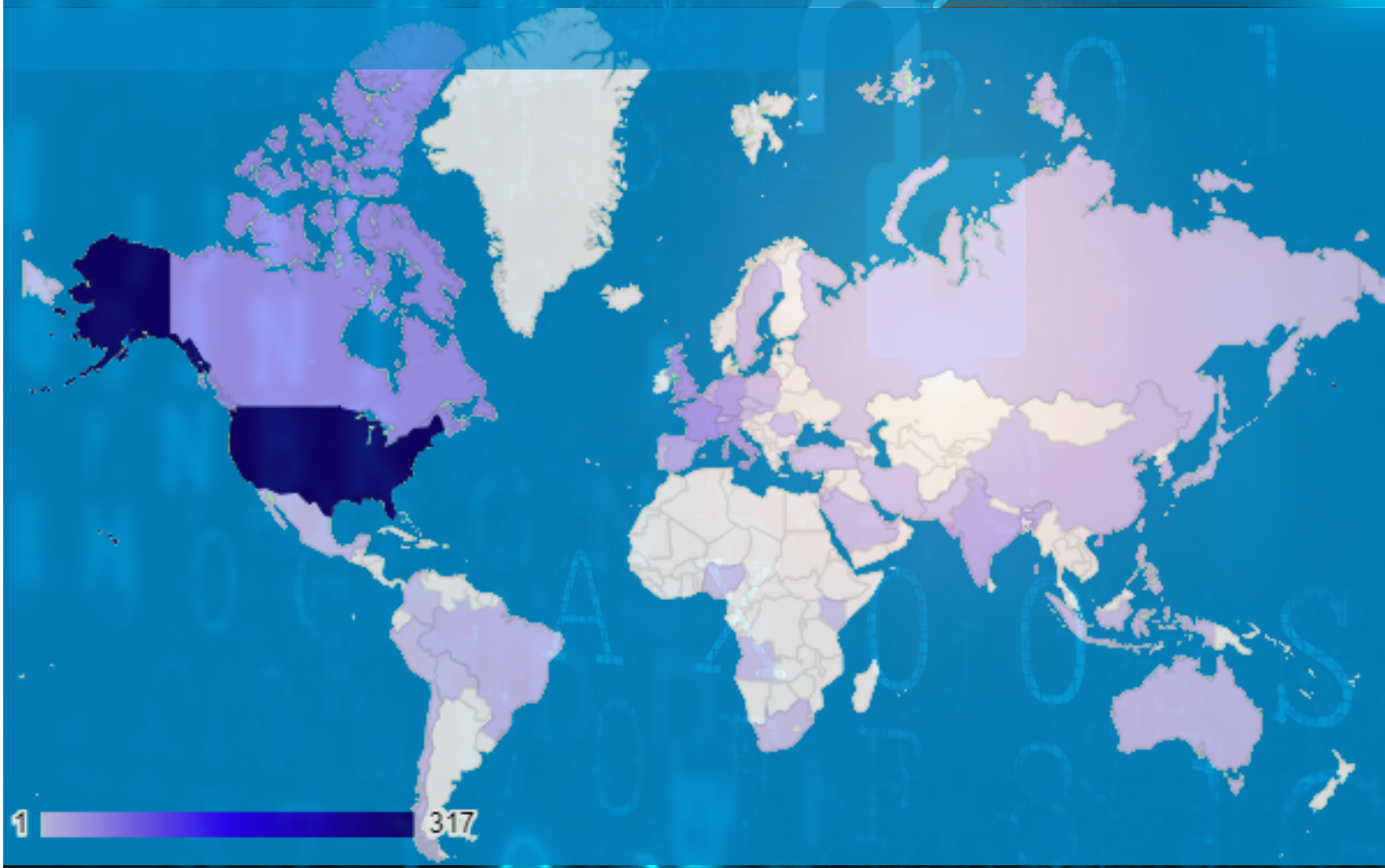
Swascan
TINEXTA GROUP

Ransomware 2021

Double extortion: Victim profiling



SOC
Swascan
TINEXTA GROUP

info@swascan.com swascan.com

Summary

Ransomware 2021

Executive Summary

In the period of time between January and May 2021, Ransomware has done nothing but confirmed itself as the primary threat in the global IT security landscape.

The spike in infections and strains that had begun to appear around the end of 2019, has only increased with a consequent evolution of TTPs (Tactics, Techniques, and Procedures) adopted and honed by different groups of Criminal Hackers, which now have evolved into full-fledged Cyber Crime cartels.

In particular double extorsion has risen to prominence.

With this in mind, Swascan's SoC as a Service Team has undertaken an analysis of the profiles of the victims targeted by Criminal Hackers.

In particular, through specific OSINT & CLOSINT researches, the data concerning the Ransomware victims who had their data published on the Darkweb has been collected and analysed.

Swascan has studied 18 Ransomware strains which now use Double extortion as their fixture and the sites where the data is published.

Avaddon	Arvin Club	Babuk	CLOP/TA505	CONTI/Ryuk	Cuba
DopplePaymer	Lorenz	LV BLOG	Mount Locker	N3tw0rm	Nefilim
Pay2Key	Pysa	RAGNAROK	Ragnar_Locker	RansomEXX	XING Team

The approach was the following:

1. Identify the Darkweb sites of the analysed Ransomware groups;

2. Identify the targeted companies which had their data published on Darkweb portals;

3. Clustering information related to victims in terms of:
   - Geographic area
   - Volume of published data
   - Turnover of affected firms
   - Strains involved

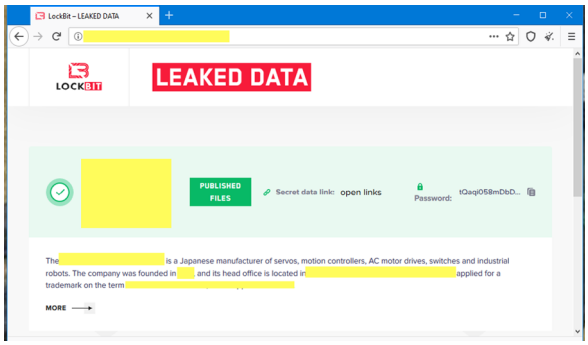


Figure 1: An example of a Double extortion website in which the data is published

Ransomware 2021

Context

Focusing on the top 8 countries in terms of the number of cases detected, it is possible to observe that the number of victims that had their data published reaches 511 cases.

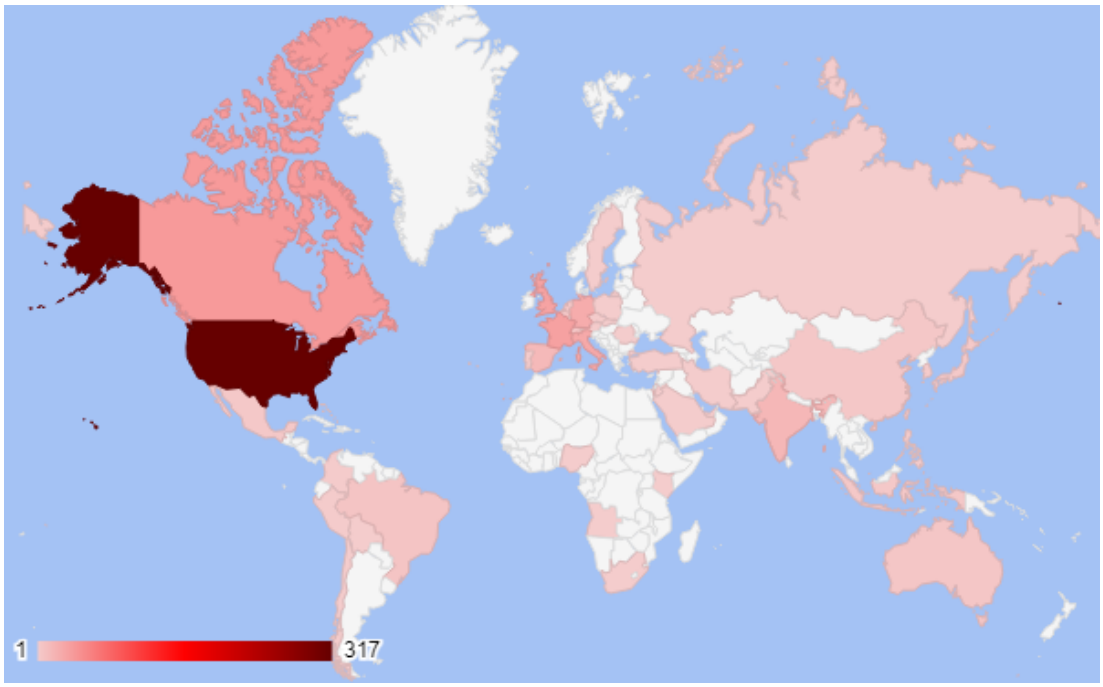


Figure 2: Geographical distribution of victims with data published in double extortion sites

As can be seen from this first chart (Figure 2), North America stands out as the absolute leader for companies with published information with 69.8% of strains hitting between the US and Canada. The former remains in the lead with 317 companies involved in the period between January 2021 and May 2021.

Canada follows with 40 instances, while the podium is closed by France with 34.

Country	Number of Ransomware victims with published data by
1. USA	317
2. Canada	40
3. France	34
4. United Kingdom	33
5. Italy	28
6 Germany	26
7 India	17
8. Spain	16

Ransomware 2021

Colonial Pipeline - the “casus belli” of the research

On May 7 2021, Colonial Pipeline, which supplies 45% of the East Coast of the United States with fuel, was the victim of a Ransomware cyberattack. DarkSide the Eastern Europe-based gang is believed – and all but confirmed - to be behind such cyber-attack.

As it often happens in this case, to prevent the spread of malware Colonial Pipeline took some of its systems offline. As a result, a pipeline transporting refined products from Houston to New York was temporarily shut down. To solve the crisis, Colonial Pipeline paid the ransom of almost 4.4 million dollars several hours after the attack and DarkSide sent the key to restore the systems.

In the meantime, however, the resulting blackout had already caused major inconveniences and unease on the daily lives of many people in the U.S.

But, as you might expect, DarkSide is not the only group of Ransomware operators on the rise.

The analysis and profiling work done by the SoC As a Service Team provides a mapping of the Double extortion phenomenon. This is done through the analysis of the data related to the companies that have had their data published by Criminal Hackers.

The cluster of targeted companies by turnover

If at the beginning Ransomware was indiscriminate and mostly targeted at individual users, today it has evolved into a real “weapon”, as demonstrated by DarkSide, capable of striking even the largest organizations.

In 2021 Ransomware gangs are increasingly focusing their business model on an economy of scale: the bigger the target, the higher the ransom. As illustrated by the chart, 57% of the companies with published data analysed by Swascan are large companies with a turnover exceeding 500 million dollars.

As a result, we can assume that smaller companies are more likely to pay the ransom (which of course will be more proportionate to the turnover of the target).

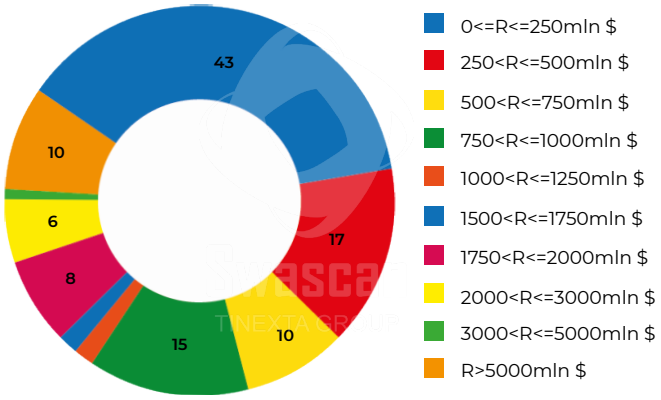


Figure 3: The cross-section of affected companies by turnover

Ransomware 2021

The most prolific Ransomware strains

Looking at the strains, once again Ryuk and its offshoot Conti lead the way, as they did for most of 2020.

Other names that stand out are DopplePaymer and Avaddon, both among the “big hitters”. In the next table (Figure 4) all the detailed data.

The “big hitters”

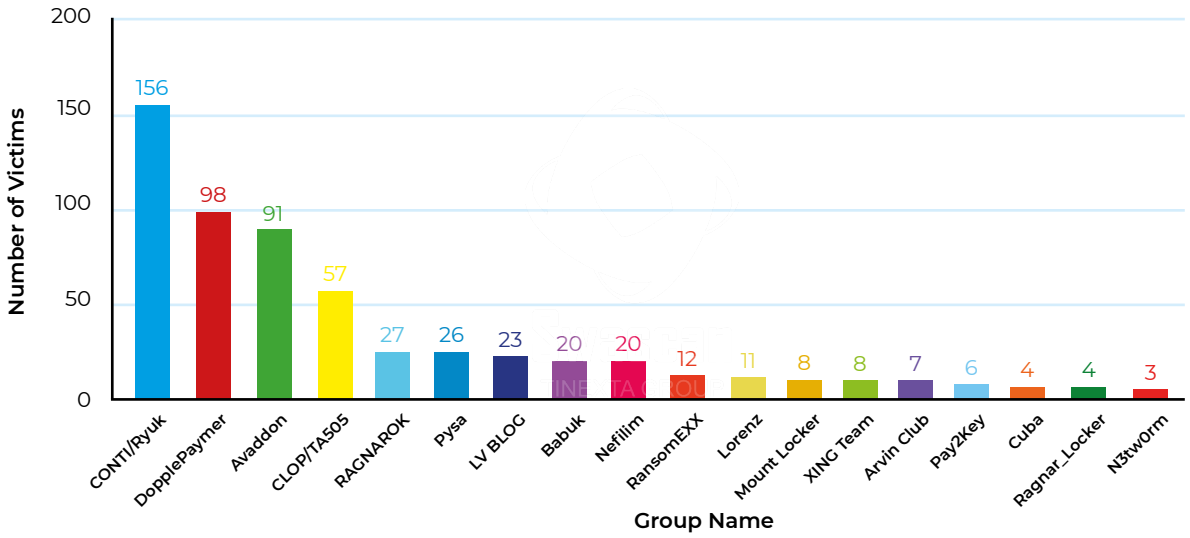


Figure 4: The most “active” Ransomwares by number of victims with data published on double extortion sites

Ransomware 2021

Timeline of Published Victims

Regarding the timeline of attacks (figure 5), March was certainly the worst month by number of published data.

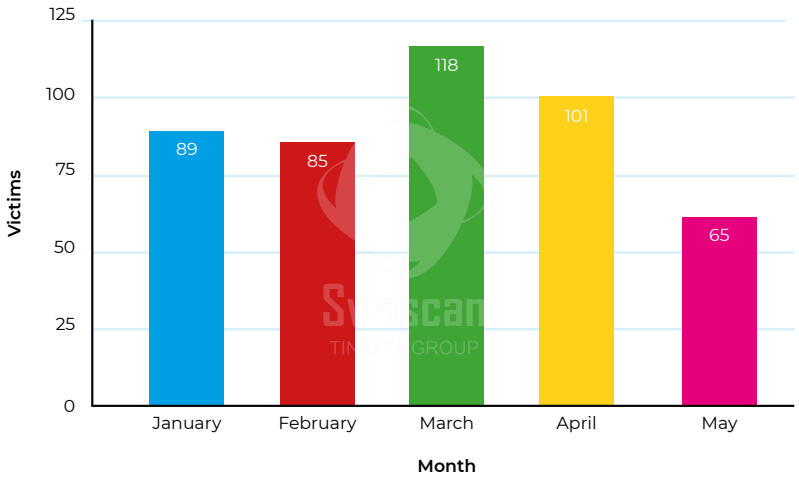


Figure 5: The number of victims distributed month by month during the period of analysis.

Data (in GB) per Month

The following chart shows the statistics extrapolated from the amount of published data (Figure 6).

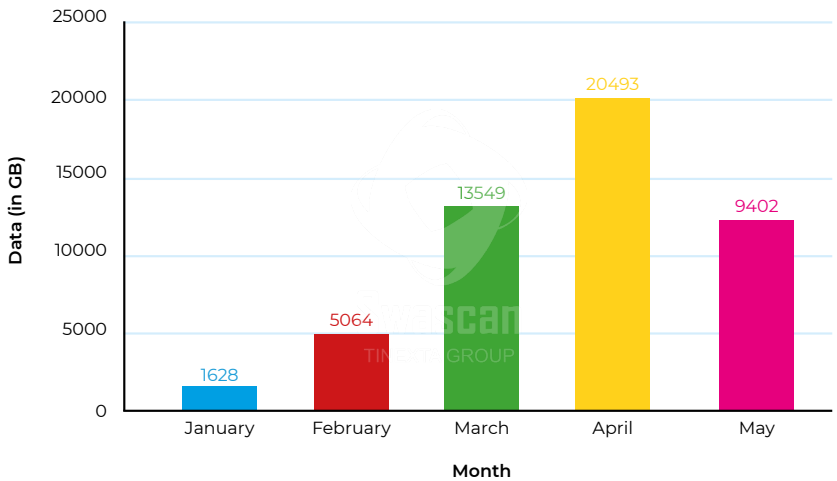


Figure 6: The amount of data (in GB) published on Ransomware gang sites on a monthly basis

It should not be forgotten that the data presented here is with the highest probability of those companies that have not paid for the ransom.

Ransomware 2021

The Strains: published data

By taking into account 14 of the 18 strains with the most complete data sets, it was possible to elaborate the table below. This reports the number of MB published for each strain and the smallest and largest data sets published for each single Ransomware. The table includes all available data (without having downloaded them for security/privacy reasons).

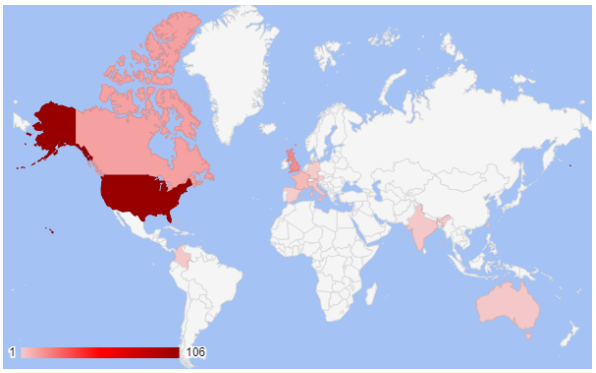
Ransomware Group	Total of data released (in MB)	Min Data Set (in MB)	Max Data Set (in MB)
Avaddon	3.404.255,46	2,36	779.060
Babuk	16.603.000	5.000	10.000.000
CLOP/TA505	5.956.924,6	500	1.126.100
CONTI/Ryuk	14.429.647,75	2,4	1.898.000
DopplePaymer	243.276,994	0,4	18.329,6
LV BLOG	1.890.000	25.000	400.000
Mount Locker	5.273.000	10.000	2.000.000
N3tw0rm	409.000	90.000	210.000
Pay2Key	14.324.000	53.000	12.400.000
Pysa	123.988,92	7,97	47.600
RAGNAROK	256.500	20.000	100.000
Ragnar_Locker	63.406,6	6,6	33.900
RansomEXX	288.904,12	430,6	119.340
XING Team	1.157.000	1.000	500.000

Ransomware 2021

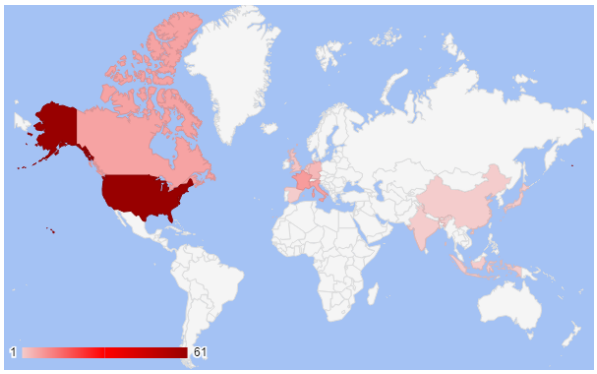
Geographical distribution of victims (TOP 6 strains)

In the course of the analysis, it was found that most strains were active in North America, particularly in the USA.
The maps below show the geographical distribution of victims by most active Ransomware strain.

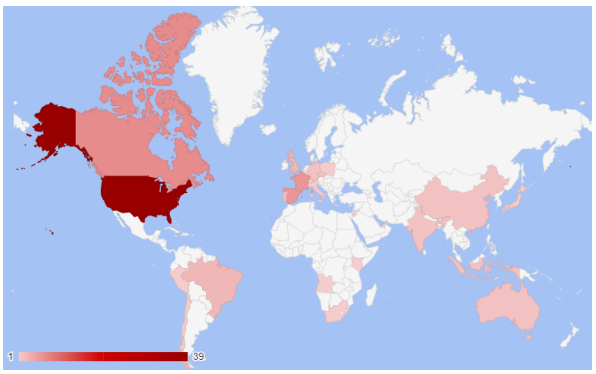
CONTI



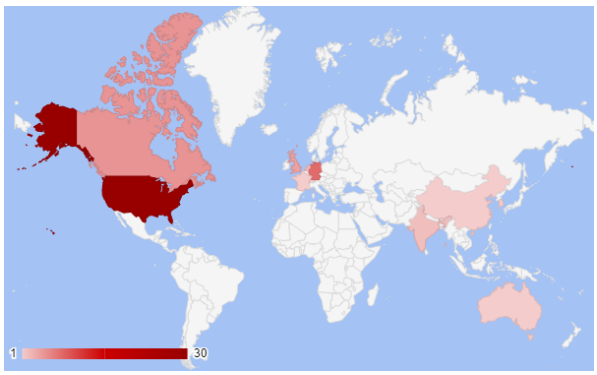
DopplePaymer



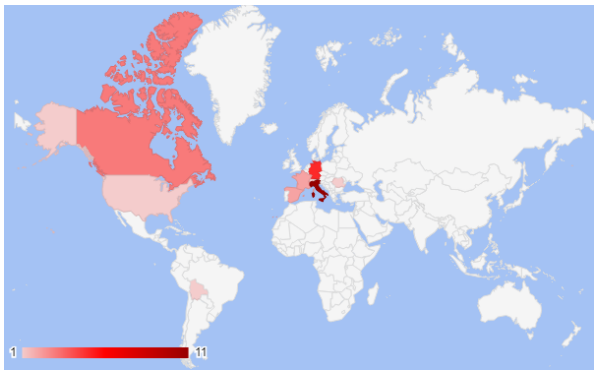
Avaddon



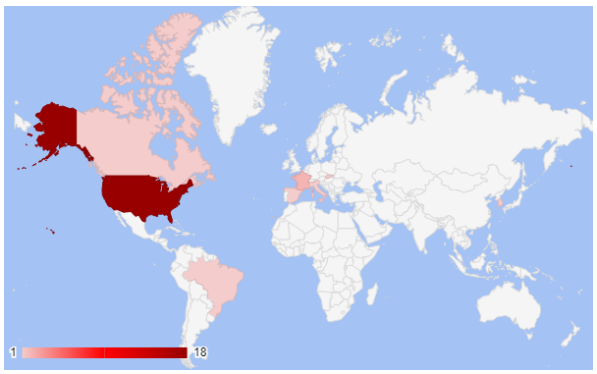
CL0P



RAGNAROK



Pysa



Ransomware 2021

How does a Ransomware attack work?

In addition to the great profit that Criminal Hackers gain from Ransomware attacks, another great advantage is the variety of techniques at their disposal to initiate an attack. The methods used by Criminal Hackers to hit their targets are countless, but they fall into two macro-categories: exploitation of vulnerabilities/technical flaws and the exploitation of the "human factor".
In fact, Ransomware often needs the help of its victims (unwitting help of course) to enter the targeted machine: this set of techniques is known as Social Engineering.
In the context of computer security, social engineering is the use of deception to manipulate people into disclosing confidential or personal information that can be used for fraudulent purposes. In other words, people can be tricked into sharing information that otherwise they would not disclose.
Common "human" attack vectors include:

Smishing

Smishing, a contraction of SMS phishing, uses text messages to induce recipients to navigate to a website or enter personal information on their device. Common approaches use authentication messages or messages that appear to be from a financial or other service provider. Some Ransomware use this technique as the first approach in the infection chain.

Vishing

Similarly to emails and SMSs, vishing uses voice mail messages to deceive the victim. The recipient of the voicemail is asked to call a number that is often spoofed to appear legitimate. If the victim calls the number, a series of actions are taken aimed at installing Ransomware on the victim's device.

Social media

Social media can be a powerful tool for convincing a victim to open an image downloaded from a social media platform or to take other actions that are compromising. The infection can spread through music, videos or other active contents that once opened infect the user's system.

Instant Messaging

IM clients can be hacked by cybercriminals and be used to distribute malware to the victim's contact list. This technique was one of the methods used to distribute Locky Ransomware to unsuspecting recipients.

Ransomware 2021

Technological/technical attack

Another type of attack vector is machine to machine. To some extent humans are involved as they might facilitate the attack by visiting a website or using a computer. However, the attack process is automated and does not require any explicit human cooperation to infect the computer or network.

Drive-By

Drive-by is so named because the victim, in order to get infected, has to open a web page with an image or an active content containing a malicious code.

Spread via shared services

Online services, such as file sharing or synchronization services, can also be used to propagate Ransomware. If the Ransomware ends up in a shared folder on a machine, the infection can be transferred to an entire office or to other connected machines. If the service is set up for automatic synchronization when files are added or modified, as it is the case with most file sharing services, a malicious virus can widely propagate in a matter of moments. It is important to be careful and consider the settings used for systems that synchronize automatically and to pay attention to sharing files with others unless knowing exactly where they come from.

System Vulnerability

Cybercriminals learn about vulnerabilities of specific systems and exploit these vulnerabilities to break in and install Ransomware on the machine. This happens more often to systems that are not patched with the latest security versions.

Malvertising

Malvertising is like drive by, but it uses ads to distribute malware. These ads may be placed on popular search engines or popular social media sites to reach a large audience (they are often very misleading banner ads). A common host for Malvertising are adult-only sites.

Supply Chain

Attacks can also come from the “extended perimeter.” By attacking the weakest links within the corporate network, hackers can hit multiple targets at once and cause serious damage – way before the company is able to detect the breach.
The risks include:

- Vulnerable third-party applications
- Out of date third-party applications and systems
- Access credentials
- Botnets
- ...

The blackmail model

After extracting and encrypting data, the most used blackmail model is the double extortion. With this the purpose of the payment is not only to decrypt data, but also to avoid leaks that could be sold to malicious third parties. In some cases, as frequently done by the Avaddon gang, if the ransom is not paid a DDOS attack is then carried out. In this case, extortion will include three threats (encrypted data, data leakage and DDOS attack).

Ransomware 2021

The defence against Ransomware threats

The best approach to counter the Ransomware phenomenon goes through the three pillars of modern Cyber Security.

Three canons have to be followed:

- **Predictive Security,**
- **Preventive Security,**
- **Proactive Security.**

Cyber Security Framework

Predictive Security

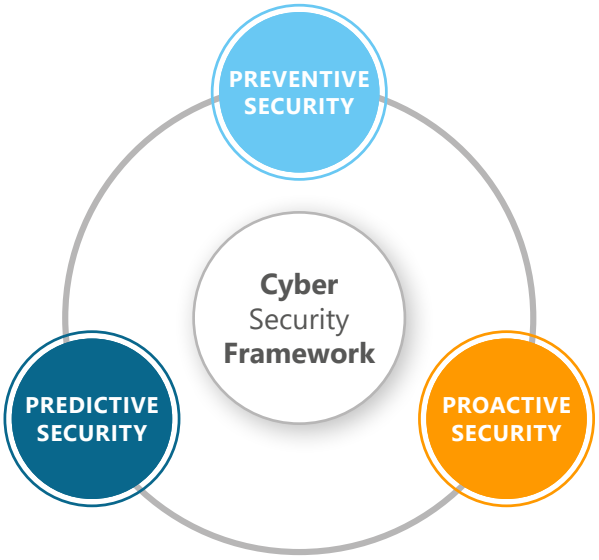
1. Identifies business threats outside the corporate perimeter taking into account the web, Darkweb and deep web
2. Researches emerging threats
3. Performs Early Warning activities
4. Provides evidence to Preventive Security
5. Indicates areas of focus for Proactive Security

Preventive Security

1. Audits and measures Cyber Risk
2. Defines remediation plans
3. Indicates the Risk exposed to the Proactive Security Layer
4. Provides areas of Investigation to Predictive Security

Proactive Security

1. Identifies cyber threats operating within the corporate perimeter
2. Counteracts and blocks cyber attacks
3. Manages Cyber Incidents
4. Provides evidence to Preventive Security
5. Indicates investigation areas to Predictive Security



Ransomware 2021

Predictive Security

Domain Threat Intelligence: The Domain Threat Intelligence activity is carried out on targets and digital identifiers related to compromised assets and emails. The activity is conducted through the search, identification and selection of publicly available information relating to domain, subdomain and compromised emails. The service does not perform any security tests on the target, it operates only on information collected at the OSINT (Open-Source Intelligence) and CLOSINT (Close Source Intelligence) level and available on databases, forums, chats, newsgroups on the Darkweb.
Specifically, based on the target domain, it identifies:

- Potential Vulnerabilities
- Vulnerability details in terms of CVEs, impacts and severity
- GDPR Impacts (CIA)
- Number of Subdomains
- Number of Potential Compromised Emails (these are only counted and not collected or processed)
- Number of Compromised Email Sources
- Typosquatting

Cyber Threat Intelligence: It is Swascan's advanced Threat Intelligence service. It performs research, analysis and collection of information from the web, Darkweb and deep web for the analyzed domain/target web. Specifically:

- Data Leaks: credentials/source/data
- Identifies ....Forum/Chat/...
- Botnets related to client, vendor and employee devices
- Botnets with credentials and login page urls
- Typosquatting/Phishing
- Surface
- Top Manager Analysis

Early Warning Threat Intelligence: this is the early warning service that daily signals the evidences that are identified and collected in the Darkweb and deep web regarding the target analyzed. Specifically:

- Botnets
- Data Leaks
- Scraping data
- Phishing data

Ransomware 2021

Preventive Security

Technological

Vulnerability Assessment: it scans websites and web applications in order to identify and proactively analyse security vulnerabilities.

Penetration Test: Penetration Testing activities are carried out by certified Penetration Testers in line with international standards OWASP, PTES and OSSTMM.

Human Risk

Phishing/Smishing attack Simulation: pit allows companies to be protected in case of phishing/smishing attacks through real attack simulations. It is possible, through a web interface, to send real simulated phishing/smishing campaigns that generate unique learning opportunities for employees.
Thanks to these simulated attacks, in the future employees will be able to identify a real phishing e-mail or smishing message and to avoid them.

Awareness: Dedicated Cybersecurity training courses in classrooms or via Webinars. Awareness activities are done for technical staff, employees and top managers.

Process - Compliance

ISO27001: ISO/IEC 27001:2013 (ISO 27001) is the international standard that describes the best practices for an ISMS (information security management system).
Since information is an asset that adds value to the organization and since nowadays most information is stored on computer, every organization must be able to guarantee the security of its data, in an environment where the risks of computer-related breaches are constantly increasing.

ICT Security Assessment: ICT Security Assessment is Swascan's proprietary methodology that allows companies to verify and measure their level of cyber risk and to assess the effectiveness of the security measures adopted.
The service provides indications and corrective actions to be taken in terms of Organization, Policy, Personnel, Technology and Control Systems.

Ransomware 2021

Proactive Security

SOCaaS: Designing, managing and maintaining a Security Operation Center can be costly and complex. Swascan SOC as a Service is the most effective, efficient, consistent and sustainable solution for business environments. The SOC as a Service with its Monitoring & Early Warning service allows to identify, detect, analyze and report cyber-attacks before they can become a real threat to the company. A team dedicated to the activity of Monitoring & Early Warning reactive to cyber threats on local networks, cloud environments, applications and enterprise endpoints. Our Security Analyst team monitors data and assets wherever they reside within the enterprise. Regardless of whether the assets are stored in the cloud, on-premises, or both. Monitoring and reporting allow you to act only when a real threat is identified.

Incident Response Management: is a set of resources and procedures that are organized and structured to ensure the proper response to an incident. In case of an IT incident, Data Breach, DDoS, Ransomware attack and/or related Data Recovery it is necessary to address and respond with a structured approach, prepared and organized to effectively and efficiently deal with the security breach and to reduce the impact on the Business Continuity level.
The objective of Incident Response is to:

- Manage the incident;
- Limit direct and indirect damage;
- Reduce recovery time and costs.

About us

Swascan

It is an innovative Cyber Security Company born from an idea of Pierguido Iezzi and Raoul Chiesa.
The first Italian Cyber Security company to own a Cyber Security testing platform and a Cyber Security Research centre of excellence; a centre that has received numerous national and international awards from the most important players in the IT market and beyond.

Since October 2020, Swascan srl has been an integral part of Tinexta Cyber (Tinexta S.P.A.), becoming an active player in the first national hub of Cyber Security, becoming an active player in the first national Cyber Security hub: not just a company, but an Italian group, a new national hub specialising in digital identity and digital security services.

Technical Contributors:

Pierguido Iezzi
Fabrizio Rendina
Valdrin Kelmendi
Pierre-Alexandre Rebuffi
Soc as a Service Team Swascan

Editing & Graphics:

Caterina Scarioni
Federico Giberti

Contact Info

Milano
+39 0278620700
info@swascan.com
Via Fabio Filzi, 2b, 20063, Cernusco sul Naviglio, MI

Ransomware 2021

Disclaimer

The research carried out by Swascan was based on sites containing data and figures published by the Ransomware groups cited in the study.

This publication does not necessarily represent the state of the art - given the transitional nature of the sources - and Swascan reserves the prerogative to update periodically.

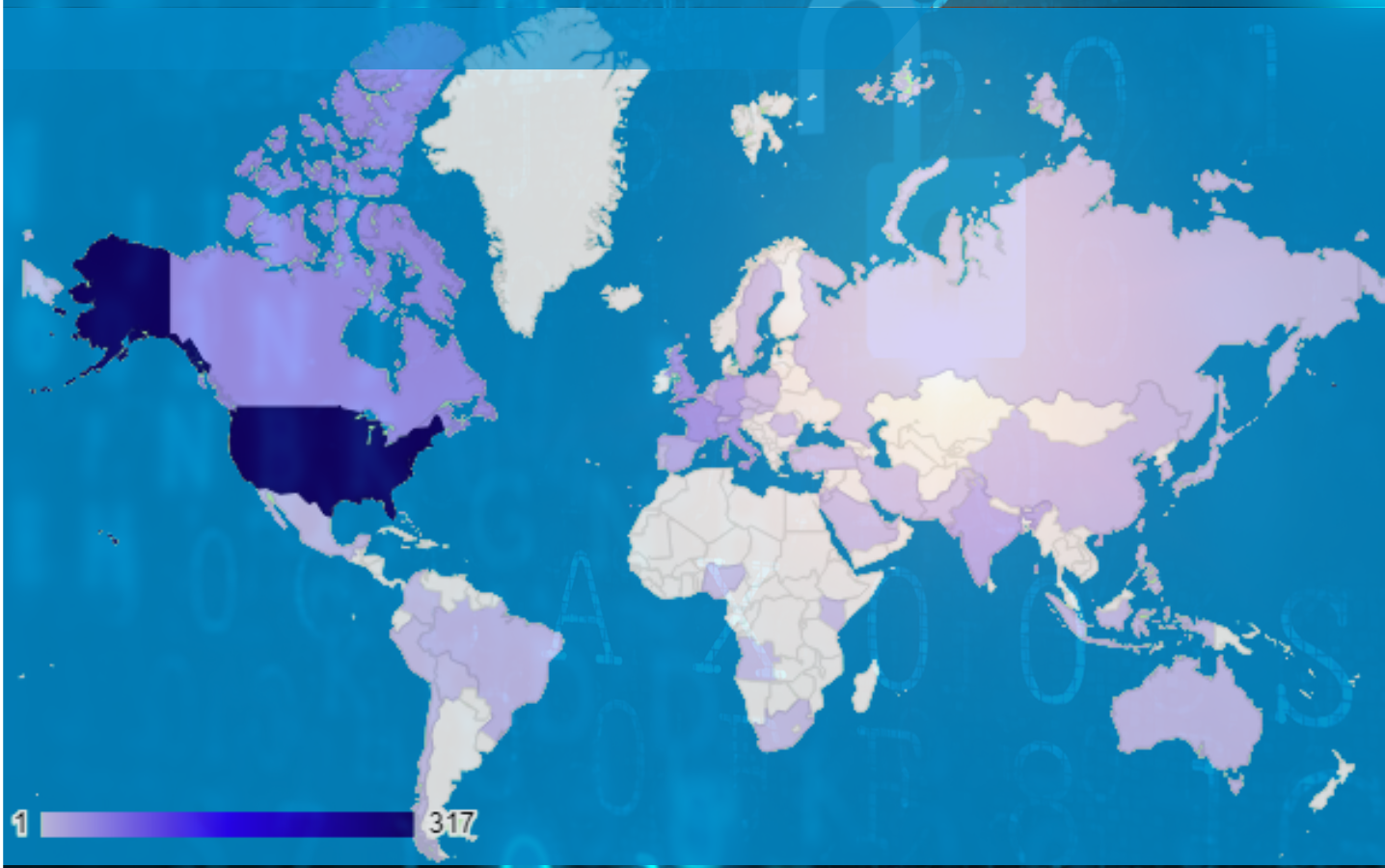
Third party sources are cited as appropriate. Swascan is not responsible for the content of external sources, including external websites referred to in this publication.

This publication is for information purposes only. It should be accessible free of charge. Neither Swascan nor any person acting on its behalf is responsible for the use that may be made of the that may be made of the information contained in this publication.

Swascan
TINEXTA GROUP

Ransomware 2021

Double extortion: Victim profiling



SOC
Swascan
TINEXTA GROUP

info@swascan.com swascan.com