# How Ransomware Groups Enhance Their Tactics with Double Extortion and Third-Party Targeting

Authors

David Hétu, PhD, Chief Research Officer
Luana Pascu, Content Writer
Christopher Ciafro, Content Writer

Flare Systems 2020

# Executive Summary

This report provides an analysis and evaluation of the state of ransomware attacks in 2020. Data analysis was conducted on dark web forums and markets, and data dumping sites launched by malicious actors active in ransomware and cyber extortion attacks. Flare Systems is the only company to have systematically indexed the attacks of double extortion ransomware groups.

Results of data analyzed show double extortion and third-party targeting are top tactics to maximize ransomware profit, and COVID-19, remote work and offline backups facilitate double extortion in ransomware attacks. Further investigations reveal malicious actors actively target small and medium businesses (SMBs) and that victims' vendors, partners and customers are collateral victims of ransomware and cyber extortion. Ransomware groups publish or auction off stolen data on their own dark web sites and some are ethically motivated. North America and Europe experienced the highest number of successful attacks, while the U.S., Canada, UK, France, and Brazil are the most targeted countries in 2020. Compromised Remote Desktop Protocols (RDP) are among major weaknesses that have caused ransomware incidents in 2020.

The report concludes  the mix of double extortion and ransom has escalated the impact of ransomware attacks, as malicious actors not only ask for ransom to release decryption keys, but also auction off the data on the dark web. There is no clear pattern in ransomware attacks, as motivations vary. Obsolete operating systems, outdated software, human error, third-parties and external threats all contribute to increasing ransomware attacks.

Recommendations include ransomware attack mitigation and data breach prevention solutions based on the MITRE ATT&CK Framework.

# Table of Contents

# 1 | The State of Ransomware Attacks in 2020

Ransomware is a type of malware that encrypts files on a computer and then asks for ransom in exchange for the decryption key. The origins of ransomware can be traced back to 1989, when it spread through floppy disks received by unsolicited mail. Both ransoms and decryption keys also had to be sent by mail.

## Malicious actors have refined their techniques & strategies

- Ransomware infections spread through spam emails and drive-by downloads. Social engineering plays a significant role in persuading victims to open **spam email attachments,** or convincing them to visit a **website that automatically infects their computers.**

- The malicious software **encrypts all files on a computer,** but it now also targets **local company backups** to ensure that victims have no alternatives but to pay the ransom.

- Ransomware identifies and instantly encrypts the most **sensitive information** causing high impact on the victim, even if it is stopped before all files are encrypted.

- Cyber criminals have specialized in either **ransomware development** or **distribution.** Known as ransomware as a service, groups work in tandem under affiliate programs and share ransom profits.

- Malicious actors have lately targeted computers with **open remote desktop connections** that use weak or leaked credentials to turn them into launch beds for large network infections.

- Individuals may be willing to pay a few thousand dollars for their files and photos, but **companies, organizations and institutions** are likely to pay millions for theirs.

- **Payment in cryptocurrencies** such as **Bitcoin** or Monero is preferred, for allegedly facilitating anonymous payments from anywhere in the world, in a matter of minutes.

- Malicious actors are **no longer targeting individuals for petty amounts of money**, but instead going after all types of companies, ranging from mom-and-pop shops to medium and large enterprises, local governments, and even hospitals and educational institutions.

# Statistics that highlight the increase in ransomware attacks

*The State of Ransomware Attacks in 2020*

Ransomware is responsible for a growing number of cyberattacks on companies, regardless of size or industry, because it is an easy way for malicious actors to make money fast.

In 2019 alone, **ransomware attacks went up by 748%**, while a single large fitness brand paid $10 million for a decryption key.

In "2019, the IC3 [Internet Crime Complaint Centre] received 2,047 complaints identified as ransomware with **adjusted losses of over USD$8.9 million**," says the latest FBI report.

Victims lost USD$3.5 billion following **ransomware attacks,** while the average number of daily **complaints from both individuals and enterprises surpassed 1,200.**

Some 41% of cyber insurance claims registered within the first six months of 2020 were ransomware-related.

> "Ransomware is the most widespread and financially damaging form of cyberattack. We have had success stories, but to be honest, it is becoming more and more complicated. This is a garden for them, and we need to change that."
>
> ***Fernando Ruiz | Acting Head of Europol's European Cybercrime Center***

# 2 | The Shift from Ransom to Double Extortion

Double extortion is a new approach adopted by ransomware groups in 2020. Double extortion attacks make backups useless, as malicious actors will now threaten to leak or auction off company secrets. Through double extortion, cybercriminals want to force victims' hand into payment.

Small and medium businesses (SMBs) appear to suffer most, with many closing their doors due to brand reputation damage, financial loss, and equipment they cannot afford to replace. In more unfortunate situations, **patients have even lost their lives due to hospital malfunctions caused by ransomware.**

Flare Systems' research confirms the **complexity and diversity of the ransomware phenomenon**, as the cybersecurity industry is no longer dealing with isolated individuals, but likely with sophisticated organized crime rings interested in ransom.

A new trend in 2020 is the shift from ransom to cyber extortion, where ransomware first engages in **data exfiltration from infected systems,** to then proceed with encryption. This affects databases, password lists, accounting spreadsheets and Office documents, among others.

### Data exfiltration is used in two types of double extortion to maximize profit

#### 1 | Put up for Auction

**Put up for auction** on ransomware group websites. The information is sold to the highest bidder, though a list of stolen files and data samples are often publicly provided.

#### 2 | Publish Online

**Published online**, encrypted. If a ransom is not paid, the **decryption keys** are revealed at a certain date and time and a list of stolen files and sample data are often provided.

## Covid-19, remote work & offline backups facilitate double extortion in ransomware attacks

The global COVID-19 pandemic has instituted a **global remote workforce** which requires access to sensitive corporate data and enterprise networks. **Double extortion ransomware cases will likely go up** over the next months. Flare Systems' research confirms double extorsion has become more prevalent in the past months.

Double extortion ransomware is a direct response to **the increased use of offsite and offline backups.** Companies have understood the growing threat of ransomware and, in many cases, have shielded themselves from most damage by restoring their files from offline backups. Disconnected from the network, offline backups cannot be attacked by ransomware. Through **data exfiltration**, malicious actors ensure the threat of leaking confidential information will lead to a ransom, whether the victim has backups or not.

# Threat Intelligence on Double Extortion Ransomware Attack Size & Scope in 2020

# 3 | Threat Intelligence on Ransomware Attack Size & Scope in 2020

Flare Systems found that vendors, partners and customers of hard targets have also been collateral victims of **double extortion ransomware.** Third-parties are attacked because they are a soft target from which data exfiltration is an easy process. In some cases, it is not even the victim's fault that data have been stolen in a ransomware attack. Although a business follows best practices and goes to great lengths to secure its networks, **third-party vulnerabilities**, business partners and clients can still compromise their security. The next session is a deep dive into **double extortion and mitigation solutions.**

## Double extortion ransomware data collection & research methodology

Flare Systems' threat intelligence team investigated major dark web forums and markets, as well as data dumping sites launched by malicious actors active in double extortion ransomware attacks to gather observations and quantitative information. The research was conducted in the summer of 2020, and Flare Systems is the only company to have systematically indexed these attacks.

Ransomware crime gangs have taken their operations to the next level, boasting on the dark web about their achievements. Flare Systems identified **nine major ransomware groups** that are using their websites to publish or auction off victims' sensitive and confidential data:

DopplePaymer MAZE

Netwalker **CLOP** **Ragnar_Locker**

Revil **PYSA MESPINOSA**

**NEFILIM** Sekhmet

To prove they are not lying, some of these groups have even **published images of the stolen repositories,** victim photos, passport screenshots, company emails, and contracts stolen from a company server.

Flare Systems collected the victims' names and used Google and LinkedIn to categorize the companies and organizations based on their sector of activity, location and size.

**Automated crawling was used to extract messages and contents of the malicious actors' websites to establish:**

## Who are the victims of double extortion ransomware?

Go to Page >

## How are successful attacks distributed geographically?

Go to Page >

## Which are the most targeted sectors?

Go to Page >

## How are successful attacks distributed across small, medium and large businesses?

Go to Page >

## How do ransomware groups choose their victims?

Go to Page >

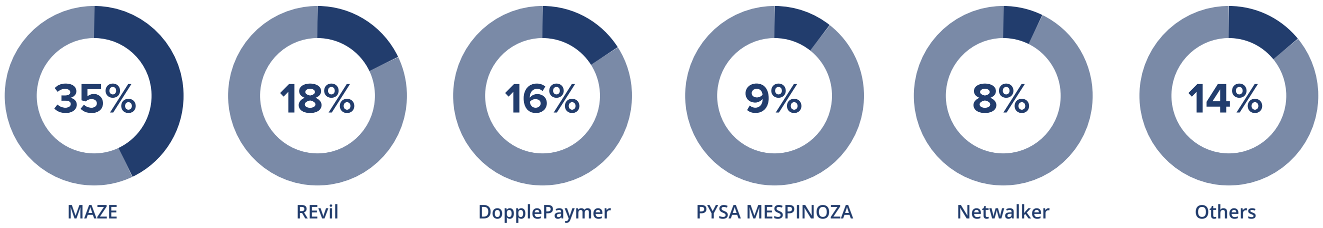
# Who are the victims of double extortion ransomware?

*Threat Intelligence on Ransomware Attack Size & Scope in 2020*

Flare Systems' threat intelligence team investigated **darknet data leaking sites associated with major ransomware groups** involved in ransom and extortion. Double extortion ransomware attacks are a new concept pioneered in December 2019 by the ransomware group MAZE. As a result, the groups surveyed in this study are relatively new to this type of attack.

The **earliest leak in our dataset dates back to February 2020.** The latest emerging double extortion ransomware group is Ragnar_Locker, who started posting leaks in June 2020. Although the number of data leaks has increased throughout the spring and summer of 2020, there is no evidence to confirm a connection to the ongoing COVID-19 pandemic.

The data show some of these groups were more prolific than others. MAZE, for example, was responsible for over 35% of breaches, followed by REvil (18%) and DopplePaymer (16%). Netwalker and PYSA MESPINOZA came close in numbers at 8% and respectively 9%. The research revealed Sekhmet, Ragnar_Locker, NEFILIM and CLOP were not responsible for a high number of breaches, as they together accounted for 14% of data breaches.



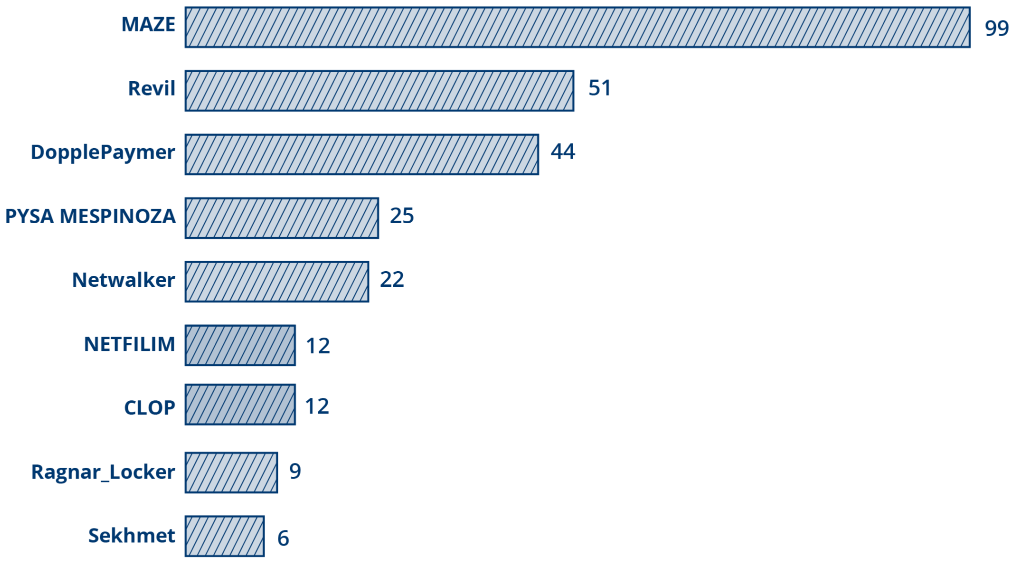


***Figure 1. Number of victims per ransomware group***

# How are successful double extortion ransomware attacks distributed geographically?

*Threat Intelligence on Ransomware Attack Size & Scope in 2020*

Ransomware attacks occur globally, yet **North America and Europe have by far registered the highest number of successful attacks.** As many as 58% were linked to companies based in North America, while 21% were related to Europe-based businesses.

## The Top Five Most Targeted Countries in 2020

| 51% | 7% | 6% | 4% | 4% |
|---|---|---|---|---|
| United States | Canada | United Kingdom | France | Brazil |

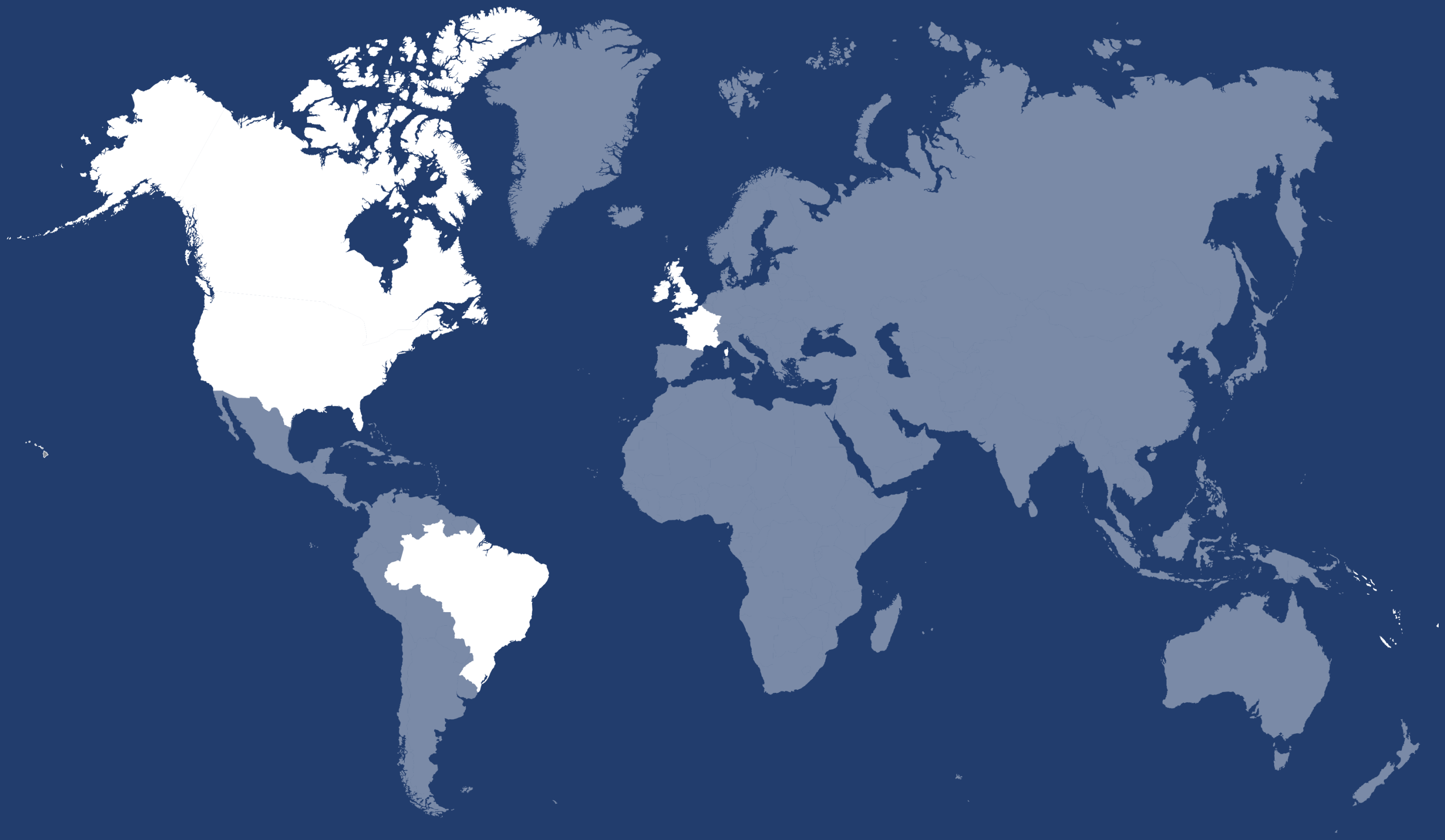


***Figure 2. Map of double extortion ransomware attacks at global level***

While the **geographical distribution of successful attacks** could simply be random, **country wealth and size** could explain some results. The U.S., U.K. and France are some of the most developed countries in the world. Canada has a much smaller economy and population, but it has a longstanding history of collaboration with the U.S. Given the interlinked economies of Canada and the U.S., companies on both sides of the border regularly communicate with each other, possibly **spreading ransomware infections** in the process. The Canada / U.S. cluster of infections is not the only one detected. Other clusters in Europe, South America, and Asia are also visible in Figure 2.

# Double extortion ransomware attack dispersion in North America

*Threat Intelligence on Ransomware Attack Size & Scope in 2020*

## The Top Most Targeted Regions in North America

| 14% | 7% | 6% | 6% |
|---|---|---|---|
| California | Ontario | New York | Texas |

The advanced economy, growing tech and entertainment scenes could be some of the reasons why California and these other states and provinces experienced the most successful attacks.

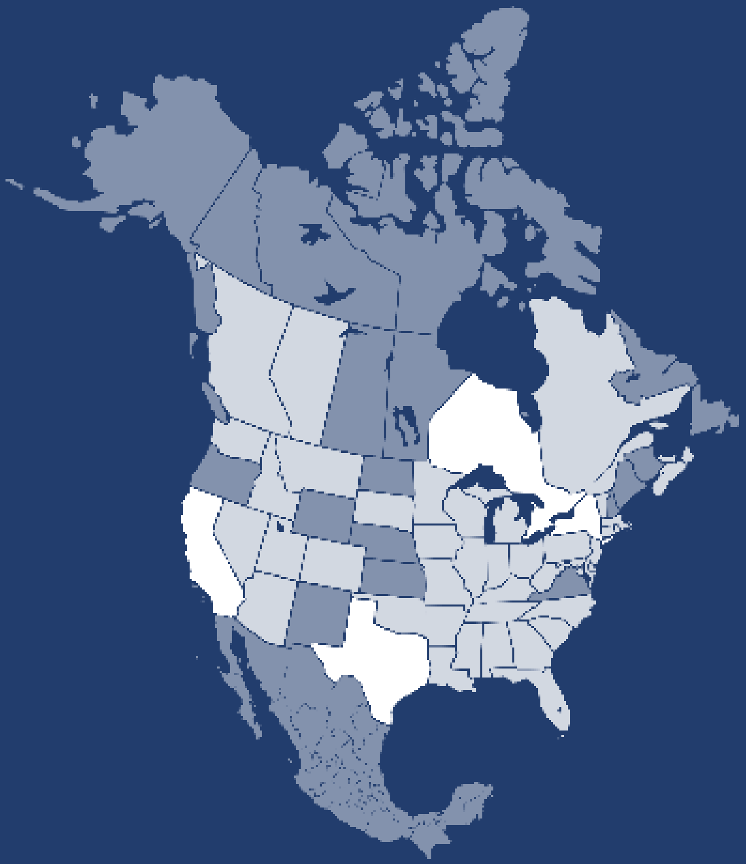


***Figure 3. Map of double extortion ransomware attacks in North America***

The **Great Lakes Region represents some 33% of total ransomware attacks** detected in North America. The Great Lakes Region includes parts of Illinois, Indiana, Michigan, Minnesota, New York, Ohio, Pennsylvania and Wisconsin, and the Canadian province of Ontario. **The Greater Chicago Region, Greater Toronto and Greater Detroit Areas** are the largest metropolitan districts in this area. The most heavily populated city in Canada, Toronto and its regional municipalities are also the fastest-growing in the country, with a booming tech sector. Malicious actors were either not interested or not successful in targeting other Canadian provinces, with only 2% of successful attacks affecting Quebec, 1% Nova Scotia, and 1% British Columbia.

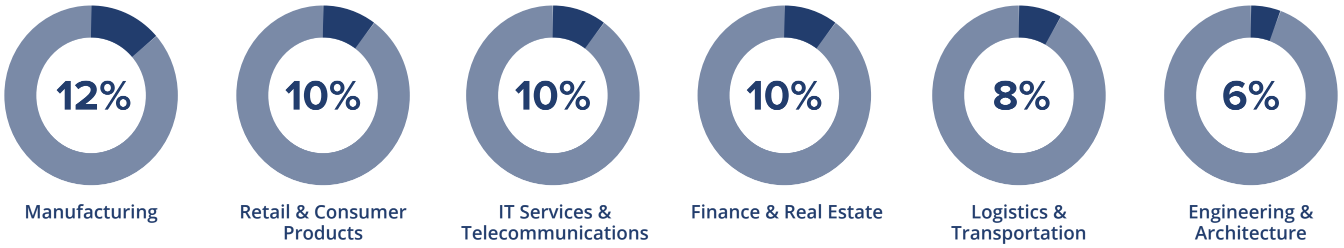
# Which are the most targeted sectors?

*Threat Intelligence on Ransomware Attack Size & Scope in 2020*

Few, if any, industries appears to be safe from double extortion ransomware groups. Companies whose data have been leaked online range from **large multinational logistics and shipping companies to small local accounting firms.** Nonetheless, certain patterns can be drawn out.

## The Most Targeted Sectors at a Global Level

At global level, companies operating in **Manufacturing saw the most successful attacks (12%),** followed by **Retail & Consumer Products (10%), IT Services & Telecommunications (10%), Finance & Real Estate (10%), Logistics & Transportation (8%),** and **Engineering & Architecture (6%).** No specific type of industry is specifically targeted within Manufacturing. Firms targeted by double extortion ransomware ranged from electronics manufacturers and textiles, to defense contractors and commercial printers.



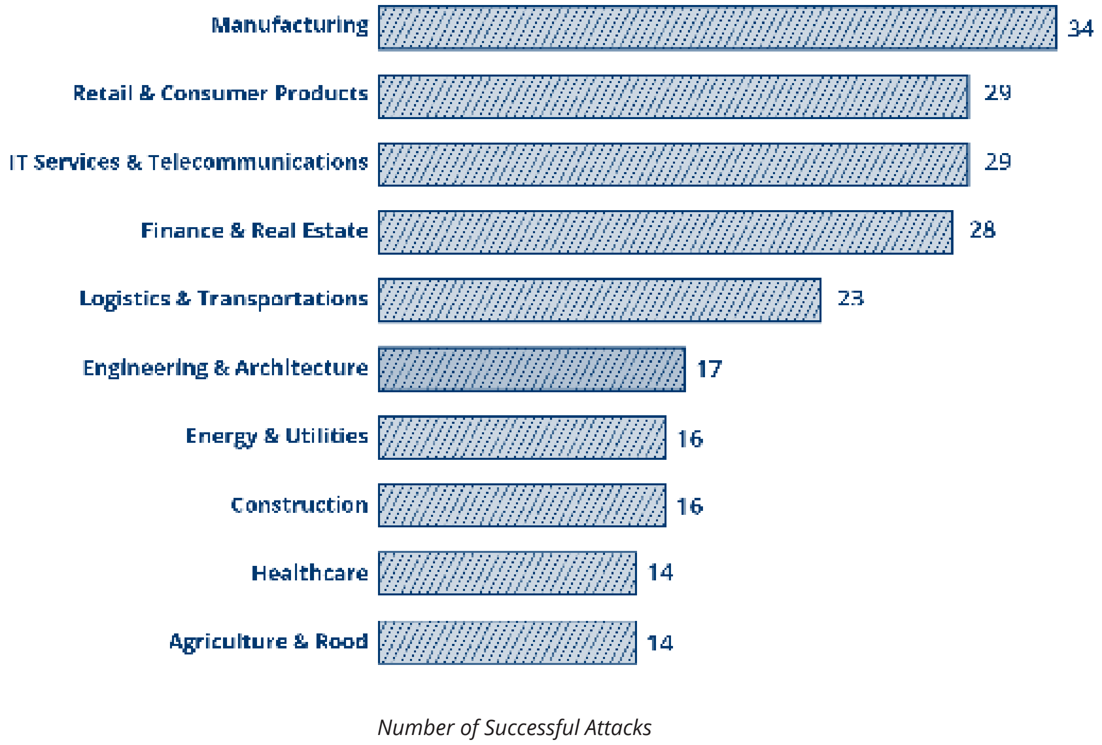


***Figure 4. Top 10 sectors targeted by double extortion ransomware at global level***

## The Most Targeted Sectors In U.S.

**The top five most targeted sectors in the U.S.** were **Retail & Consumer Products (15%), Manufacturing (11%), IT Services & Telecommunications (11%), Finance & Real Estate (10%),** and **Construction (7%).** Compared to global numbers, Retail & Consumer Products and Construction experienced most attacks in the U.S.

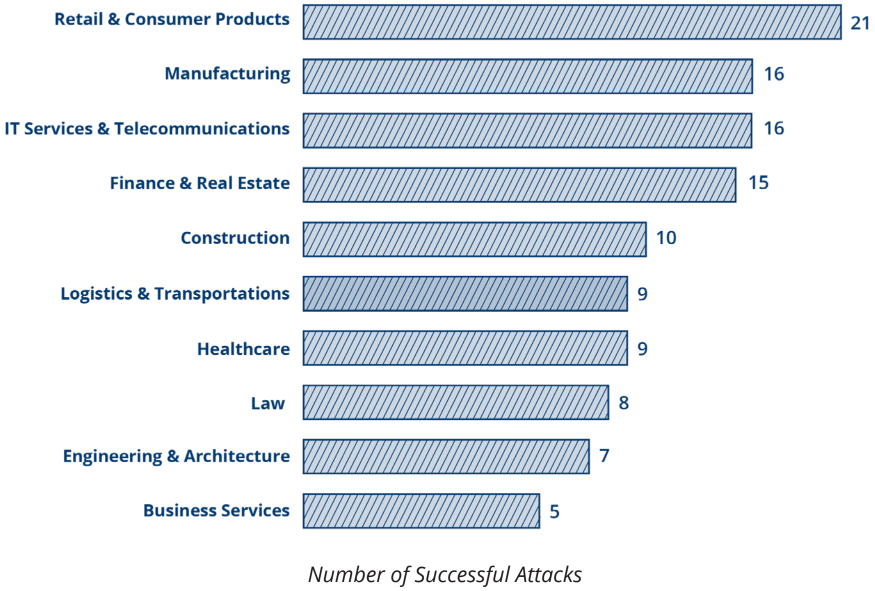


***Figure 5. Top 10 sectors targeted by double extortion ransomware in the U.S.***

## The Most Targeted Sectors in Canada

**Manufacturing and Finance & Real Estate were the main sectors in Canada** that fell victim to double extortion ransomware attacks. An overwhelming majority of companies are based in Ontario, followed by Quebec, Nova Scotia, and British Columbia. Finance & Real Estate are more targeted in Canada than at global level, suggesting that malicious actors may be targeting this sector more intensely in that country.

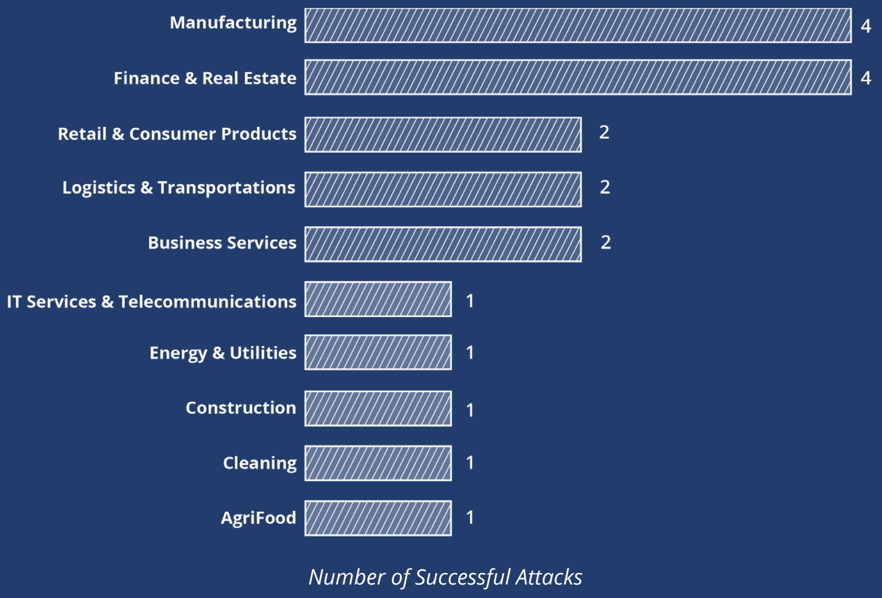


***Figure 6. Top 10 sectors targeted by double extortion ransomware in Canada***

# How are successful attacks distributed across small, medium & large businesses?

*Threat Intelligence on Ransomware Attack Size & Scope in 2020*

Ransomware groups have a differential level of success depending on the size of the companies they target. Companies that have  between **50 and 200 employees** seem to be the **preferred target of malicious actors**, accounting for over two-thirds of double extortion ransomware attacks.

The lowest number of attacks was experienced by the smallest and largest companies, likely because the firms with the smallest number of employees can't provide much value for malicious actors, while the largest might have more robust security. The cost-benefit ratio likely causes a preference for middle-sized companies. Another reason to target middle-size companies is their connection with larger corporations.

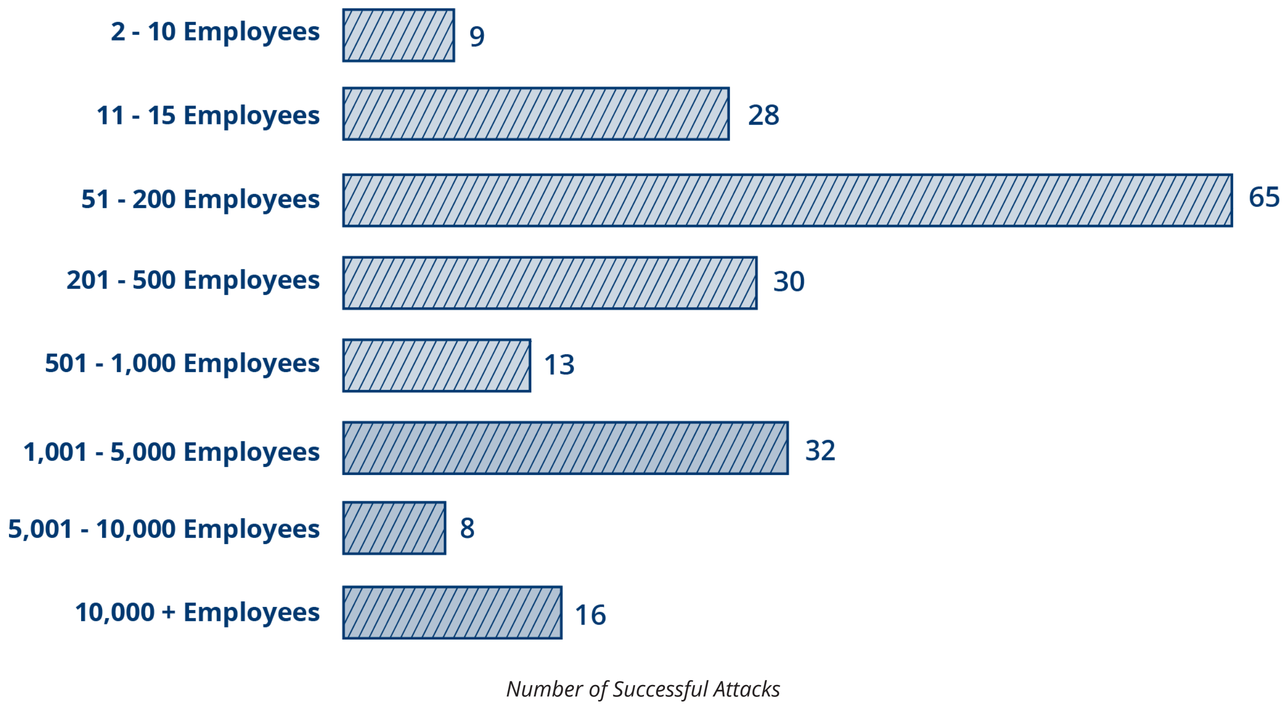
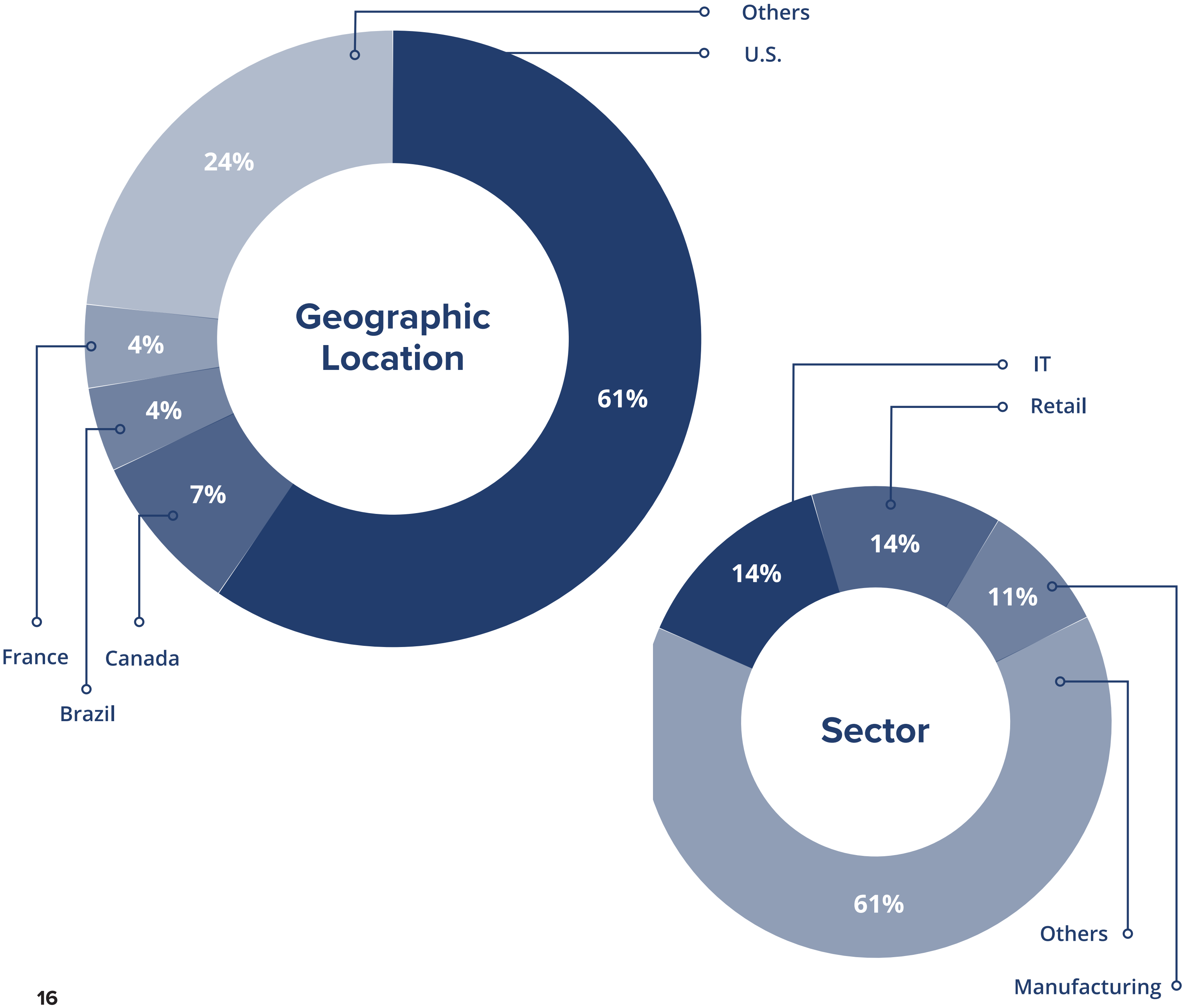


***Figure 7. Double Extortion Ransomware attack breakdown by company size***

Each ransomware group seems to have slightly different motivations, beyond sheer profit. While some have **political and socio-economic interests,** others appear to enjoy the chaos and confusion they create.

## Maze Ransomware Group | Financial Motivation

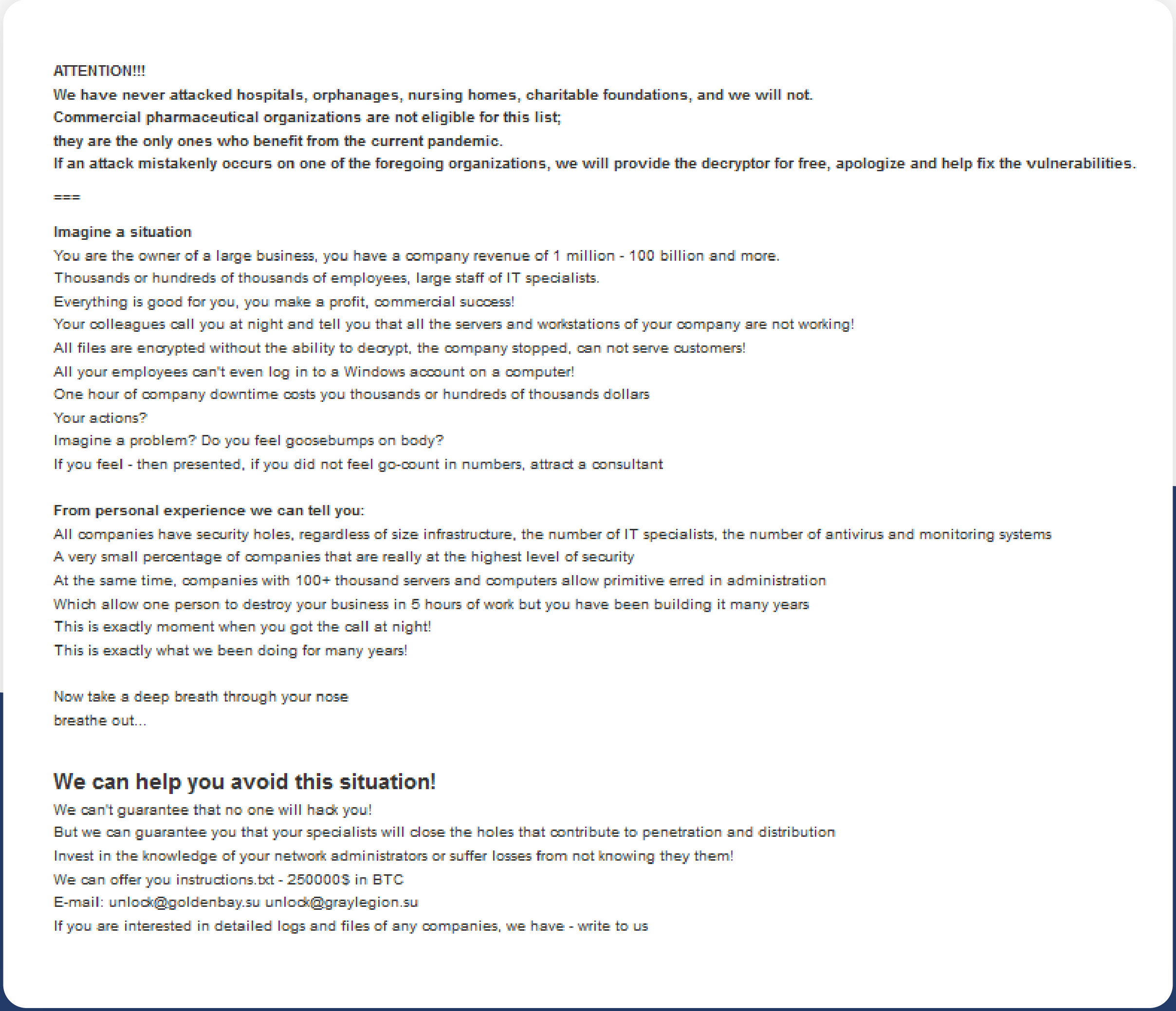
As far as the number of victims is concerned, **MAZE** is one of **the most prolific ransomware groups.** Although the group pioneered the double-extortion tactic, MAZE announced in a recent press release that they have shut down operations and that there is no cartel.



## CLOP Ransomware Group | Ethical Motivation

**CLOP ransomware group** seems to operate on a **relatively strict code of ethics**. According to their main page, CLOP argues there is an ethical component in how victims are chosen, as it is specifically going after companies that make money off unfortunate situations such as the **COVID-19 pandemic**. From the beginning, the group makes it very clear that hospitals, orphanages, nursing homes and charitable foundations have never been on the target list. Should any of these **institutions fall victim to an attack**, the group commits to providing a **decryption key for free** and to fix all vulnerabilities. Commercial pharmaceutical organizations, however, are not exempt from attacks, because CLOP believes they are taking advantage of the pandemic to make money.

CLOP claims the information it holds was publicly accessible on the Internet and did not have even basic protection. On the website, the group believes it is doing a good deed "protecting" these companies from "stupid schoolboys or dangerous punks." Yet these companies are then ungrateful and don't want to pay ransom.



ATTENTION!!!
**We have never attacked hospitals, orphanages, nursing homes, charitable foundations, and we will not.**
**Commercial pharmaceutical organizations are not eligible for this list;**
**they are the only ones who benefit from the current pandemic.**
**If an attack mistakenly occurs on one of the foregoing organizations, we will provide the decryptor for free, apologize and help fix the vulnerabilities.**

===

**Imagine a situation**
You are the owner of a large business, you have a company revenue of 1 million - 100 billion and more.
Thousands or hundreds of thousands of employees, large staff of IT specialists.
Everything is good for you, you make a profit, commercial success!
Your colleagues call you at night and tell you that all the servers and workstations of your company are not working!
All files are encrypted without the ability to decrypt, the company stopped, can not serve customers!
All your employees can't even log in to a Windows account on a computer!
One hour of company downtime costs you thousands or hundreds of thousands dollars
Your actions?
Imagine a problem? Do you feel goosebumps on body?
If you feel - then presented, if you did not feel go-count in numbers, attract a consultant

**From personal experience we can tell you:**
All companies have security holes, regardless of size infrastructure, the number of IT specialists, the number of antivirus and monitoring systems
A very small percentage of companies that are really at the highest level of security
At the same time, companies with 100+ thousand servers and computers allow primitive erred in administration
Which allow one person to destroy your business in 5 hours of work but you have been building it many years
This is exactly moment when you got the call at night!
This is exactly what we been doing for many years!

Now take a deep breath through your nose
breathe out...

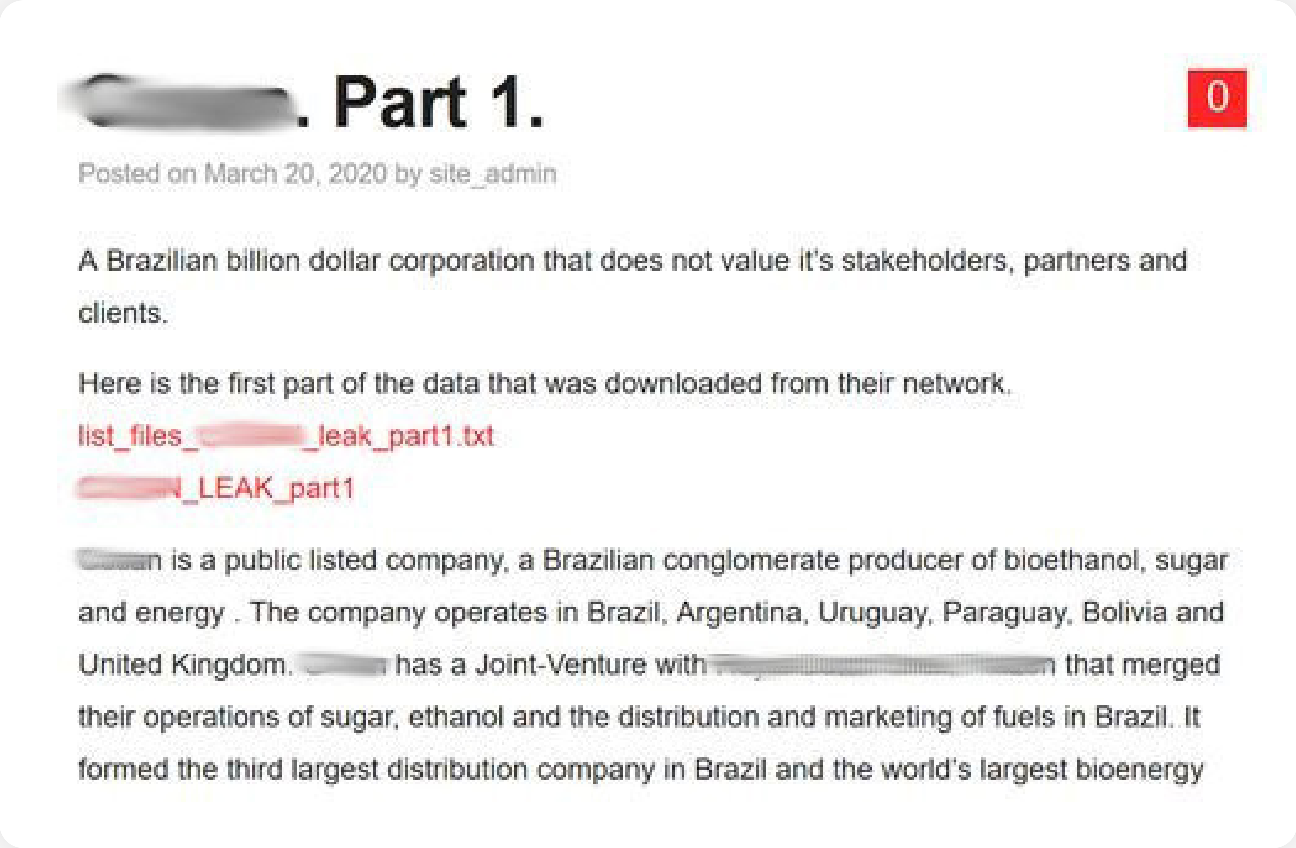
**We can help you avoid this situation!**
We can't guarantee that no one will hack you!
But we can guarantee you that your specialists will close the holes that contribute to penetration and distribution
Invest in the knowledge of your network administrators or suffer losses from not knowing they them!
We can offer you instructions.txt - 250000$ in BTC
E-mail: unlock@goldenbay.su unlock@graylegion.su
If you are interested in detailed logs and files of any companies, we have - write to us

***Figure 8. Screenshot of CLOP's announcement***

## NEFILIM Ransomware Group | Social Motivation

**NEFILIM** has a **similar ideology to CLOP**, but tends to target large conglomerates in **Energy & Utilities, Transportation & Logistics, Pharmaceuticals, and Fashion**, in essence companies with representation in multiple countries. As far as geography is concerned, the group targets companies with headquarters in Brazil, India, U.S., Australia, Switzerland and Germany. These victims were targeted for allegedly disrespecting their workers, shareholders, or the general public in some way.

According to its leak site, NEFILIM has targeted a corporation for its allegedly **unethical corporate practices,** including potential usage of slave labour. The personal data of corporate officials are included for the sake of political motivations. NEFILIM is a strong protester against the increasing disparity in wealth between the working and owning classes.



[redacted]. Part 1.

0

Posted on March 20, 2020 by site_admin

A Brazilian billion dollar corporation that does not value it's stakeholders, partners and clients.

Here is the first part of the data that was downloaded from their network.

list_files_[redacted]_leak_part1.txt

[redacted]_LEAK_part1

[redacted] is a public listed company, a Brazilian conglomerate producer of bioethanol, sugar and energy . The company operates in Brazil, Argentina, Uruguay, Paraguay, Bolivia and United Kingdom. [redacted] has a Joint-Venture with [redacted] that merged their operations of sugar, ethanol and the distribution and marketing of fuels in Brazil. It formed the third largest distribution company in Brazil and the world's largest bioenergy

*Figure 9. Screenshot of NEFILIM's announcement*

## DoppelPaymer Ransomware Group | Searching for Vulnerabilities

**DoppelPaymer** has targeted **North American companies** with middle to large work forces, out of which most were located in the U.S. Affected sectors include Supply Chain, Pharmaceuticals, and Essential Service Providers, though at least one military institution was also targeted.

Based on screenshots posted on the group's website, the companies that fell victim to DoppelPaymer's attacks may have used **outdated operating systems** such as Windows 7 and Windows XP. Given the fact that Windows XP, for instance, was released in 2001 and Microsoft no longer delivers security updates or any technical support, **malicious actors may abuse vulnerabilities** in the OS that are unlikely to be fixed with a security patch.

The group's posts are often cynical, making puns in relation to the names or practices of the business targeted.

## REvil Ransomware Group | Political Motivations

**REvil** has named its page "Happy Blog." The group **stole as much as 100GB of company data** from one business alone, and claims "Absolutely all servers and working computers of the company are hacked and encrypted."

Stolen data that has been leaked online, but also auctioned off, includes databases, employee and customer information, working documentation, correspondence, financial data, audit results, bank account passwords, counterparty databases, technical solutions and engineering developments.

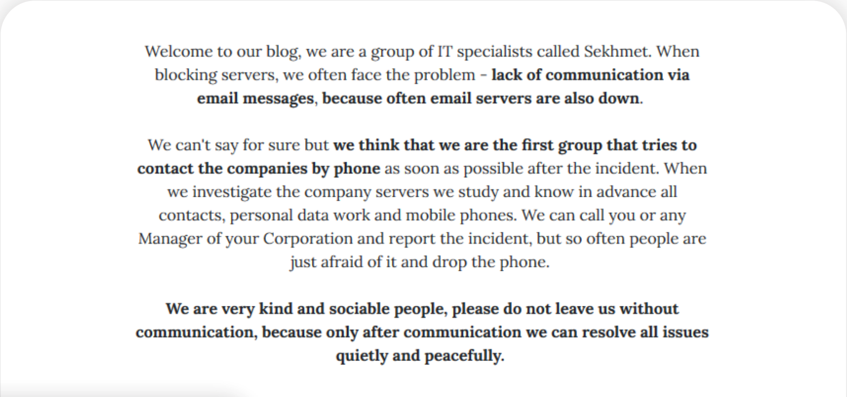
**The ransomware group appears political in the decision-making process.** For example, according to a "press release" it posted, REvil claims to have **stolen personal and private data of current U.S. President Donald Trump:**

> **"The next person we'll be publishing is Donald Trump. There's an election race going on, and we found a ton of dirty laundry on time. Mr. Trump, if you want to stay president, poke a sharp stick at the guys, otherwise you may forget this ambition forever. And to you voters, we can let you know that after such a publication, you certainly don't want to see him as president. Well, let's leave out the details. The deadline is one week."**
>
> ***-REvil ransomware group***

## Sekhmet Ransomware Group | Financial Gains Motivation

**Sekhmet is interested in financial gains**, boasting with the media coverage received for its hacks. **This type of media coverage** is likely to **impact the victims' brand and reputation** more severely than if the attack had remained confidential.

The group is very different in its approach, as it first **reaches out to the victims by phone.** Surprised that companies drop their calls, the group states they "are very kind and sociable people, please do not leave us without communication, because only after communication we can resolve all issues quietly and peacefully".



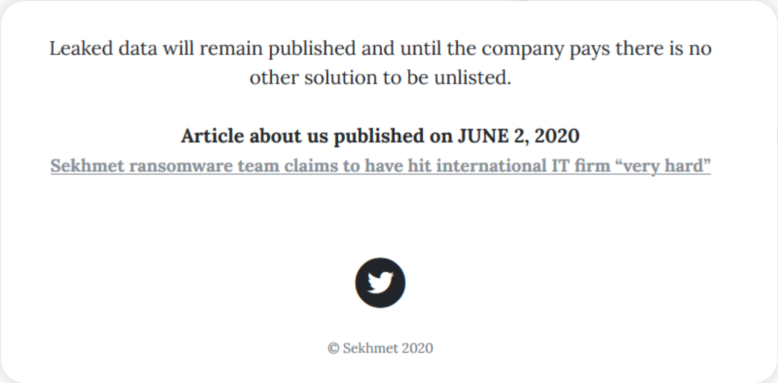
Welcome to our blog, we are a group of IT specialists called Sekhmet. When blocking servers, we often face the problem - **lack of communication via email messages, because often email servers are also down.**

We can't say for sure but **we think that we are the first group that tries to contact the companies by phone** as soon as possible after the incident. When we investigate the company servers we study and know in advance all contacts, personal data work and mobile phones. We can call you or any Manager of your Corporation and report the incident, but so often people are just afraid of it and drop the phone.

**We are very kind and sociable people, please do not leave us without communication, because only after communication we can resolve all issues quietly and peacefully.**

© Sekhmet 2020

***Figure 11. Screenshot of Sekhmet's announcement***



Leaked data will remain published and until the company pays there is no other solution to be unlisted.

**Article about us published on JUNE 2, 2020**

Sekhmet ransomware team claims to have hit international IT firm "very hard"

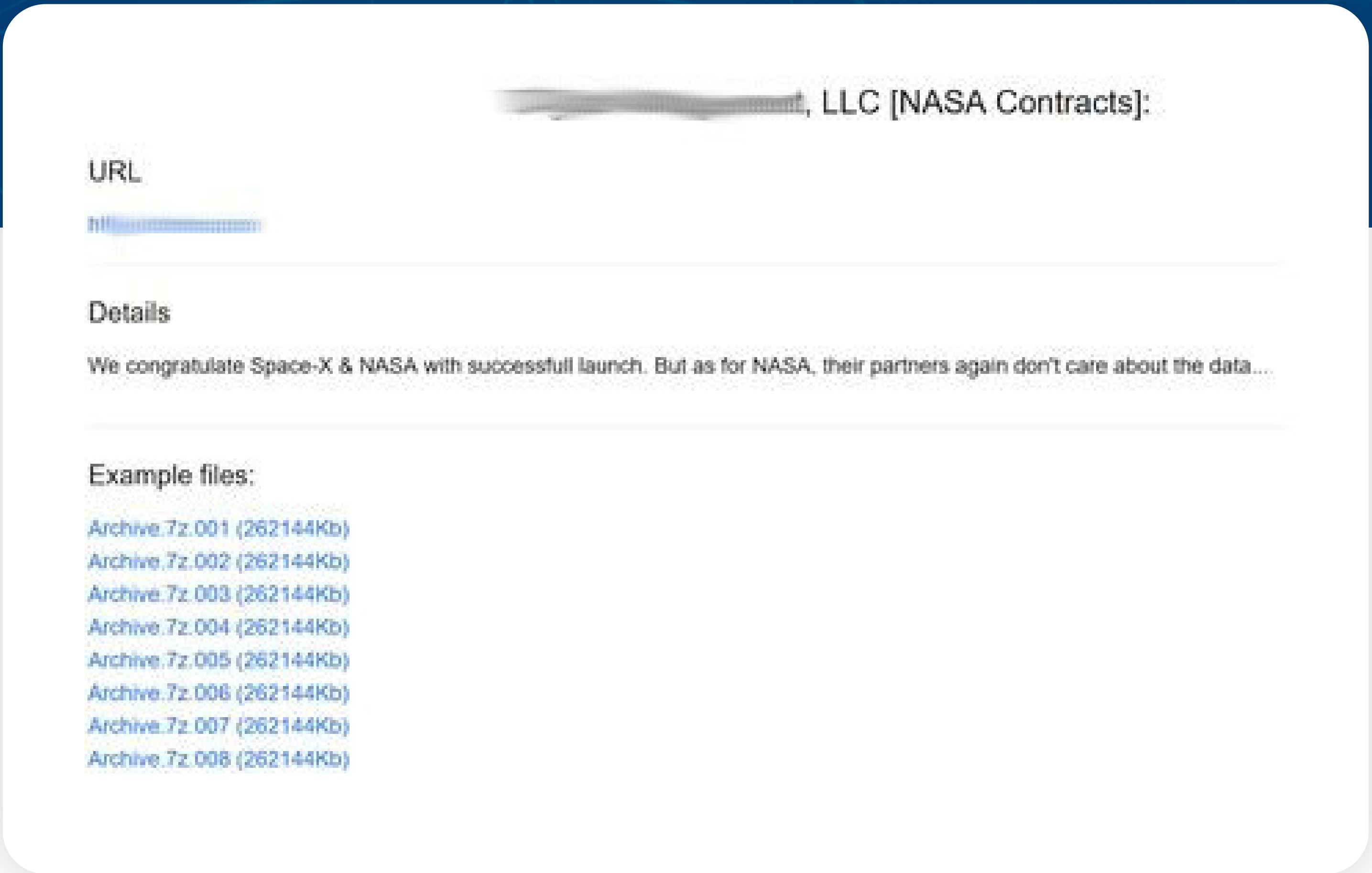
© Sekhmet 2020

***Figure 10. Screenshot of Sekhmet's announcement***

As far as understanding how ransomware groups choose their victims, **Flare Systems' investigation has not revealed a single characteristic common to all victims.** The use of obsolete operating systems and outdated software, as well as weak or leaked credentials could explain some of the success the groups had. Political reasons, personal vendettas, or questionable practices also appear to play a role in infections. However, there is probably a random effect playing out with ransomware groups, perhaps aiming for specific companies, but ending up infecting others as **collateral damage.**

# 4 Third-Party Role in Double Extortion & Ransomware Attacks

A reason to target smaller companies could be linked to their position in the supply chain of other, major corporations or conglomerates. Some of the **targeted companies have a rich customer portfolio** which includes Fortune 1000 listed companies.



[redacted], LLC [NASA Contracts]:

URL

[redacted]

Details

We congratulate Space-X & NASA with successfull launch. But as for NASA, their partners again don't care about the data...

Example files:

Archive.7z.001 (262144Kb)
Archive.7z.002 (262144Kb)
Archive.7z.003 (262144Kb)
Archive.7z.004 (262144Kb)
Archive.7z.005 (262144Kb)
Archive.7z.006 (262144Kb)
Archive.7z.007 (262144Kb)
Archive.7z.008 (262144Kb)

For example, while DopplePaymer might not have been interested in the company itself, it used it as patient zero to reach bigger names such as NASA.

***Figure 12. Screenshot of DopplePaymer's announcement***

Companies used offline backups as a second line of defense to mitigate breaches, should antivirus and other security software not detect an attack. With **cyber extortion, a failure in security software** means that backups, even those offline, are no longer effective to **mitigate breaches.** This increases company reliance on security software to detect even the latest ransomware. However, **antivirus software can be the source of attacks** and may be too slow to learn about new malware.

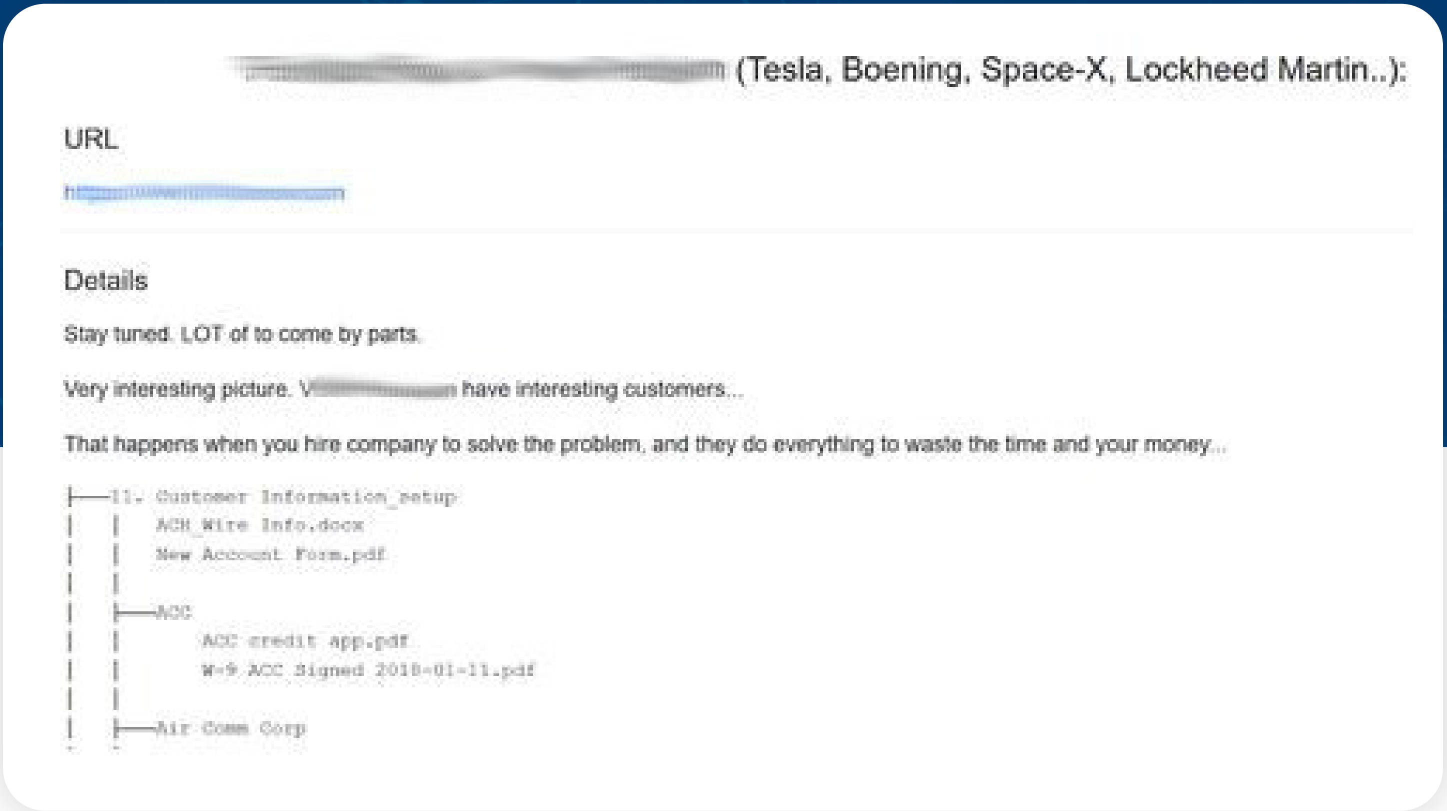
The mix of cyber extortion with ransom increased the importance of external threats. Ransomware used to target corporate networks, but companies that developed mature security procedures and enforced their industry's best practices could limit the number of breaches suffered. Companies have little control over their data, **since ransomware groups started targeting third-parties** such as vendors, partners and even regulators. Businesses can request **third-parties implement certain security standards**, but these are difficult to enforce and verify before a breach.

Large companies are most at risk given the **weak security** in their **third-party networks**. A famous company is more likely to gain media attention, even though it was not the main target. **Third-party attacks are difficult to prevent,** because businesses must share confidential information with their partners, vendors and suppliers. The larger a company grows, the more third-parties it is likely to interact with in its daily business activities.

**Confidential information leaks** to competitors is another major issue. Cyber extortionists can threaten to sell the data to competitors, who also have access to download it if made public. This can jeopardize a company's market position in a way that ransomware never could before. A 21st century goldmine, trade secrets, strategies and client list leakage can severely impact a company's value and operations.

**Third-party breaches** affect victims' reputation, brand image and civil responsibilities. A company that has fallen victim to a third-party breach may have to explain **how third-parties were chosen and vetted,** and **which measures were taken to ensure data integrity.** When no answers are provided, customers may question business decisions and could lose trust in the company.

In 2020, research shows ransomware attacks have grown in complexity while malicious actors operate as organized crime groups. Depending on distribution methods, ransomware attacks follow different paths across the **MITRE ATT&CK framework**, but always end with **data encrypted** (T1486) in the **impact** phase.



[redacted] (Tesla, Boening, Space-X, Lockheed Martin..):

URL

h[redacted]

Details

Stay tuned. LOT of to come by parts.

Very interesting picture. V[redacted] have interesting customers...

That happens when you hire company to solve the problem, and they do everything to waste the time and your money...

```
├──11. Customer Information_setup
│   │   ACH_Wire Info.docx
│   │   New Account Form.pdf
│   │
│   ├──ACC
│   │       ACC credit app.pdf
│   │       W-9 ACC Signed 2018-01-11.pdf
│   │
│   ├──Air Comm Corp
```

A similar case occurred with a company that listed **Tesla, Boeing and Lockheed Martin** as clients.

***Figure 13. Screenshot of DopplePaymer's announcement***

# 5 | Ransomware Attack Mitigation Based on MITRE ATT&CK Framework

Flare Systems' Firework solution mitigates ransomware attacks. Below is a detailed explanation of how Firework operates according to the mitigation section of the MITRE ATT&CK framework.

## Threat Intelligence Program (M1019)

A threat intelligence program seeks to develop accurate and comprehensive information on attack vectors, as well as on the nature of attacks likely to target a company. **Flare Systems' Firework solution** collects millions of data points on a daily basis from all corners of the criminal underground. Its robots index discussion forums, illicit marketplaces, chat rooms and paste sites to extract the best possible intelligence on **ransomware distribution methods and attacks.** Firework leverages **automated tagging and classification** to identify discussions and generate intelligence about ransomware that is in development or in the wild.

### Description of Ransomware Behavior

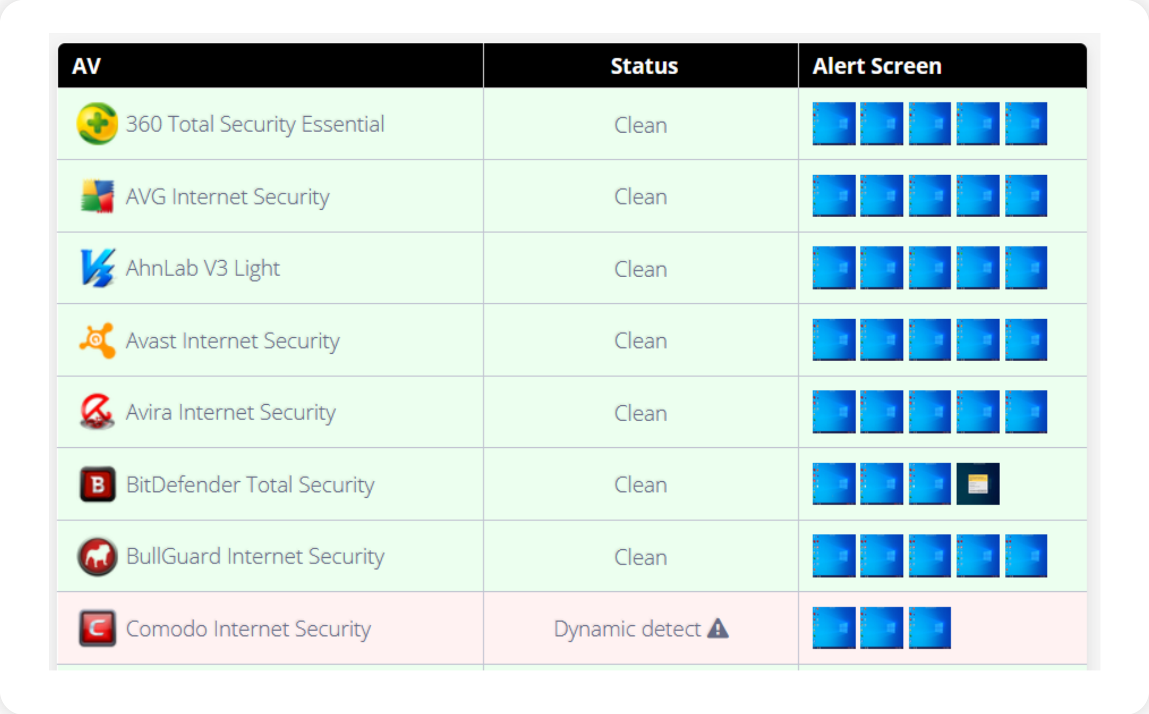
The table below presents the type of intelligence that Firework collects on ransomware, as well as examples of posts by malicious actors that fit each type.

| Intelligence | Example |
|---|---|
| Distribution methods | "LAN Spreading. As this ransomware is designed with companies in mind, it can spread from one computer to another in the same LAN or even from a VM to its host if writing permissions are present" |
| Types of vulnerables platforms | "Works well and it has been thoroughly tested from Windows 7 and up" |
| Active evasion techniques | "Kill other antivirus. At the moment the ransomware can cripple AVG and Malwarebytes"<br>"Anti-VM: Client can be set to gracefully exit in case it detect it is running in a virtual analysis environment" |
| Attack methods | "Erase shadow copies created by third party products"<br>"Added built-in RootKit so the ransomware is no longer visible in task manager during encryption" |

The threat intelligence can be imported into other security tools and used as a signature to detect infections, before they exfiltrate confidential information or encrypt files and backups. It can also be integrated with other phases of the **MITRE ATT&CK framework.**

Malicious actors post links to virus checks of their ransomware. This information helps security teams understand if their security software can detect specific ransomware. Then they can alert their antivirus company about including a new threat in the virus signatures and behavior profiles.

Most ransomware developers in the wild publish screenshots to reveal the antivirus solutions they can circumvent and those that detect their malware.



| AV | Status | Alert Screen |
|---|---|---|
| 360 Total Security Essential | Clean | ■■■■■ |
| AVG Internet Security | Clean | ■■■■■ |
| AhnLab V3 Light | Clean | ■■■■■ |
| Avast Internet Security | Clean | ■■■■■ |
| Avira Internet Security | Clean | ■■■■■ |
| BitDefender Total Security | Clean | ■■■▣ |
| BullGuard Internet Security | Clean | ■■■■■ |
| Comodo Internet Security | Dynamic detect ⚠ | ■■■ |

*Figure 14. Screenshot published by a ransomware developer*

**Firework detects third-party leaks caused by cyber extortion.** It creates alerts based on company, executive and domain names that are fuzzy matched to the content collected daily. By building a list of identifiers and creating alerts in Firework, companies can protect themselves and others with **real-time data leak notifications.** Third-party breach awareness enables companies to start their investigation sooner, prepare a public statement, and disable compromised credentials and passwords.

To overcome data leaks and breaches, companies need effective technology to **reduce digital risk and fraud.** A user-friendly, comprehensive platform, Firework automates dark, deep and clear web monitoring, and provides security teams with **real-time actionable intelligence to manage risks.** It leverages AI technology to scan the criminal underground for sensitive data leaks and provides more visibility into the digital footprint. Flare Systems' technology detects phishing attacks, prevents account takeover and financial fraud, and manages reputation risks.

**Compromised Remote Desktop Protocol (RDP) endpoints** brought about the highest number of ransomware incidents in enterprises in 2020. Companies that fall victim to ransomware attacks generate collateral damage that could affect their business partners. It is important for them to protect their assets and infrastructure not only by following basic security guidelines, but also by understanding the threat landscape.

### *General best practices to prevent ransomware attacks*

While it's fair to say there is no silver bullet in security nowadays, companies can still follow a few basic guidelines to **prevent ransomware attacks**, such as performing regular software updates and avoiding obsolete systems that no longer receive updates, security patches or technical support. Besides RDP compromise, **spear phishing emails remain a top threat for organizations.**

**To prevent data breaches**, companies should train their employees to not click on links that appear suspicious and not download email attachments from unverified sources. They should always double check the email address from which the message was received and look for typos or domain errors, as malicious actors have improved their methods to easily impersonate other companies.

Considering the remote workforce is gaining ground worldwide, employees should avoid using a public WI-FI connection when accessing sensitive corporate information or servers. If this situation cannot be avoided, employees should use a Virtual Private Network (VPN) to protect their connection and immediately inform their security team. Keeping regular backups of all company information to restore the system and files in case of a ransomware attack is another good practice.

Double extortion and ransomware victims should reach out to law enforcement immediately and avoid negotiators that facilitate payments, as the U.S. federal government is in the midst of introducing **sanctions for companies that encourage ransomware payments.**

These recommendations are summed up in the **MITRE ATT&CK mitigation framework.**

- Antivirus/antimalware (M1049)
- Application isolation and sandboxing (M1048)
- Behavior prevention on endpoint (M1040)
- Code signing (M1045)
- Execution prevention (M1038)
- Filter network traffic (M1037)
- Network segmentation (M1030)
- Update software (M1051)
- User training (M1017)

# About Flare Systems

Since 2017, Flare Systems has been developing AI-driven technologies that automate fraud detection and prevention. Firework offers an easy-to-use platform that gets you the right information before risks become unmanageable. Reduce digital risk and fraud with Firework, the digital risk protection (DRP) platform that automates your dark, deep and clear web monitoring to deliver real-time actionable intelligence.

Book a Demo

www.flare.systems
hello@flare.systems

1751 Rue Richardson, Unit 3.107
Montreal, Quebec, H3K 1G6