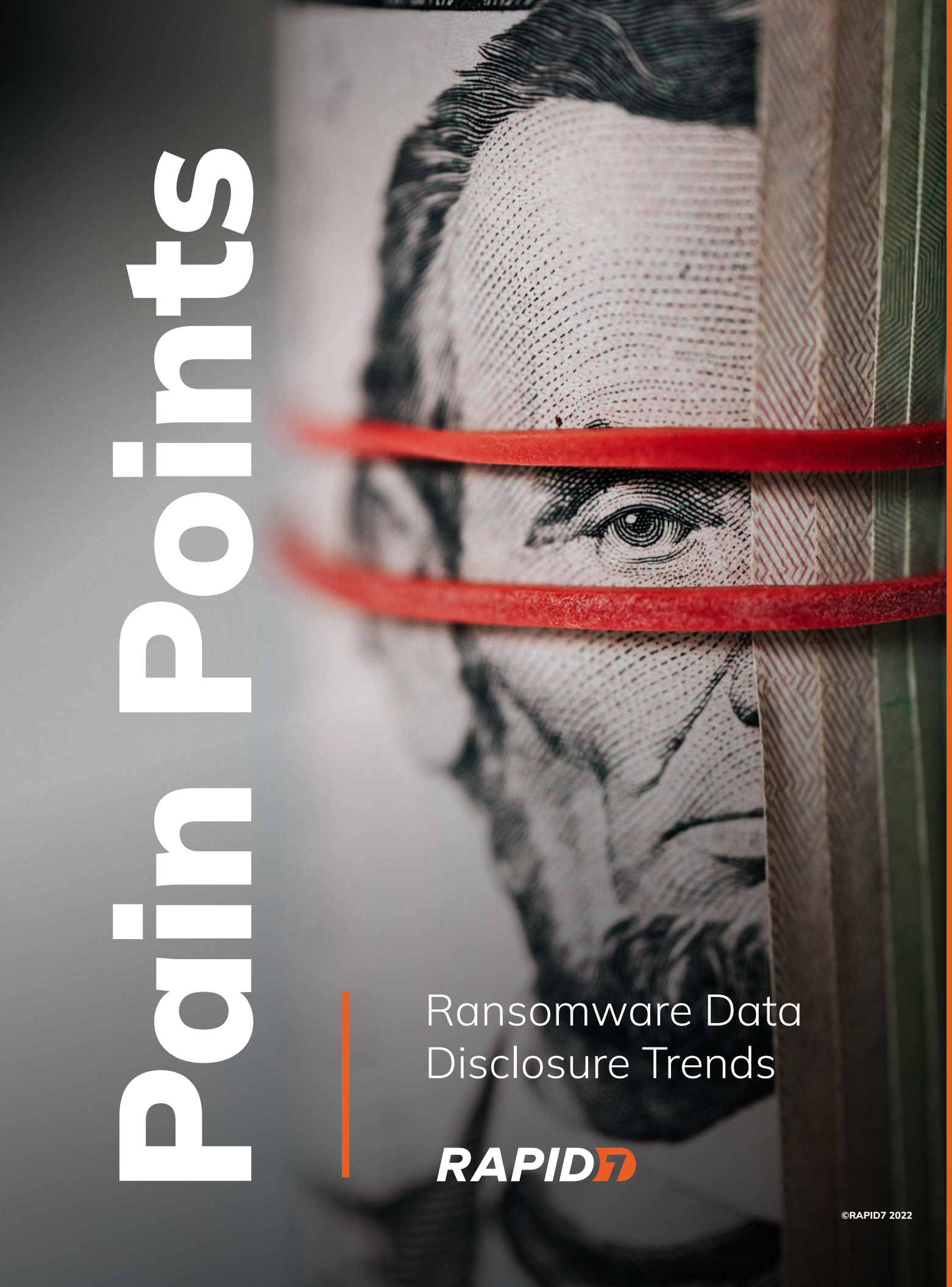
Pain Points



Ransomware Data Disclosure Trends

RAPID7

EXECUTIVE SUMMARY

This report investigates the trend, pioneered by the Maze ransomware group, of double extortion. In particular, we examine the contents of initial data disclosures intended to coerce victims to pay ransoms.

Rapid7 analysts investigated 161 separate data disclosures between April 2020 and February 2022 and identified a number of trends in the data.

FINDINGS

Among the findings: There are general trends in data leaked that vary only slightly, but three sectors display unique patterns: Financial Services, Healthcare, and Pharmaceuticals.

12% of leaks were of intellectual property, which is rare in general, except in pharmaceuticals, where it was included in **43%** of the disclosures investigated.

The collapse of the Maze ransomware group in November 2020 led to the emergence of several smaller groups that recaptured the lost market share.

Targets in Financial Services are more likely to have customer information disclosed than other types of data.

Leaked data varied by threat actor group. While Conti leaked financial information in **81%** of the incidents included, Cl0p included financial information in only **30%** of included incidents, generally preferring to leak employee information **70%** of included incidents.

63% of data leaked was financial, the most commonly leaked data in general, followed by customer/patient data **48%.**

INTRODUCTION AND METHODS

This paper sheds new light on ransomware attacks, particularly the initial data disclosure layer of "double extortion." Rapid7 analysts reviewed a data sample consisting of all ransomware data disclosure incidents that were reported to customers via industry-specific alerts in our Threat Command threat intelligence platform (TIP). Rapid7 analysts also drew upon both threat intelligence coverage and institutional knowledge of cybercriminal communities, particularly Russian-speaking ones, for context and background. Unless otherwise noted, this knowledge base and the sample of data disclosure incidents are the sources for this paper.

This sample is not exhaustive but serves as a selection of incidents that analysts deemed significant and credible enough to report to customers not directly impacted by them. The time frame for these incidents was from April 2020 to February 2022. Data disclosure became more common during this period, following the Maze ransomware group's pioneering of the technique.

CONTENTS

What is Ransomware Data Disclosure, and Why do Criminals do it?

Many ransomware attackers targeting enterprise networks do not simply encrypt files to hold for ransom. They may instead spend time – sometimes as much as multiple weeks – surreptitiously collecting and exfiltrating files from a compromised network after achieving sufficient access, but before encrypting files with ransomware payloads. Some ransomware attackers conducted pre-encryption data collection before the earlier, pioneering adoption of data disclosure by the Maze ransomware group. Maze's influence made disclosure of that collected data more common in ransomware incidents, as the ransomware attackers who also collected data often intended to sell it to other criminals before Maze demonstrated another way to monetize that data. The goal was to ensure thorough monetization of network compromises via both ransom payments and sales of stolen data.

The growing adoption of backups as one of the best lines of defense against ransomware file encryption has likely influenced this trend. Backups give victims the ability to restore their files without paying ransoms, thereby relieving much of the coercive pressure that ransomware attackers aim to exert on them. Backups can protect victims from the file encryption layer of double extortion, but they cannot shield victims from the coercive pressure of the data disclosure layer of double extortion.

In any event, this dwell time of silent data collection and exfiltration before the encryption of files serves as an opportunity for protectors. This delay in the encryption of files can give network protectors an opportunity to detect the compromise before attackers inflict more damage to victims by encrypting files.

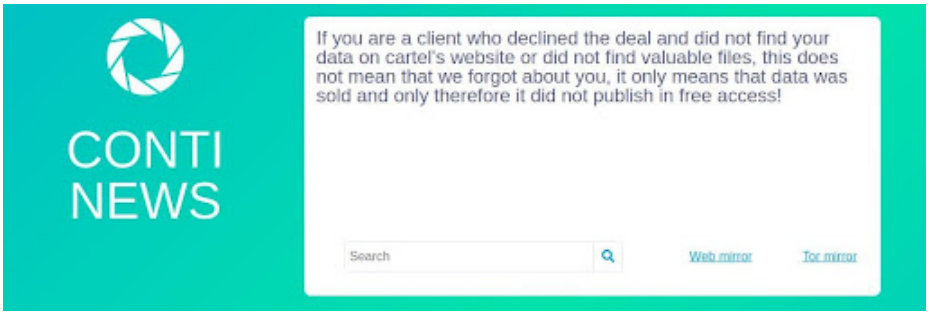


FIGURE 1 In some incidents, ransomware groups may opt to sell data privately, rather than disclose it publicly for the purpose of extortion.

Ransomware data disclosures typically come in two stages. A first-stage disclosure involves the release of a sample of compromised data in order to make the threat credible to victims, and to demonstrate the damage that further disclosure would inflict upon them. By this point, the attackers have often given the victim a first opportunity in private to pay the ransom, and the victim initially refused, prompting the attacker to place additional coercive pressure on them in a public manner. A second-stage disclosure occurs if and when attackers disclose or sell more or all of the previously unreleased data in their possession because the victim still refused to pay the ransom for that layer of the attack.

As an illustrative example, the unusually detailed preface to a data disclosure by REvil included below indicates that the ransomware attackers responsible for it put thought into the specific types of files that they included. They considered the implications that this disclosure would have for the compromised company's relationships with vendors, customers, and employees and chose the files to disclose on that basis.

Similarly, another group cited the reputation damage that a compromised company would suffer from the disclosure of specific types of files that it disclosed. It chided the compromised company for allegedly failing to use security solutions and its employees for alleged negligence.

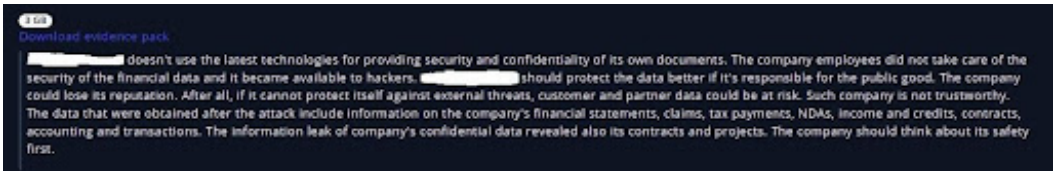
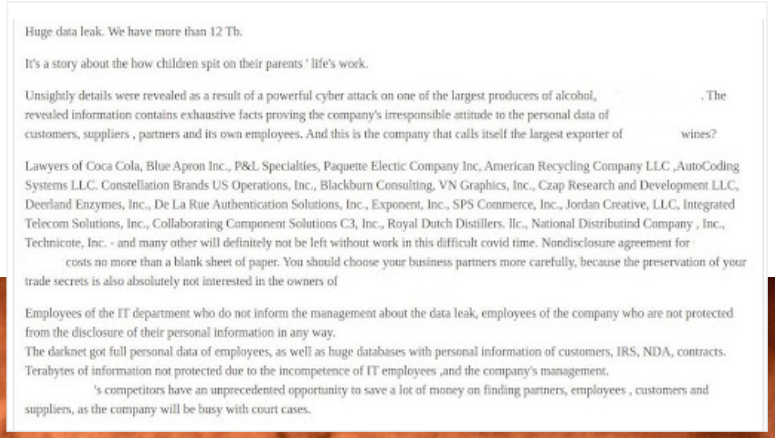


FIGURE 2 The Marketo ransomware group chides a compromised company for allegedly inadequate security and highlights specific types of files that would damage its reputation via their disclosure.


Huge data leak. We have more than 12 Tb.

It's a story about the how children spit on their parents ' life's work.

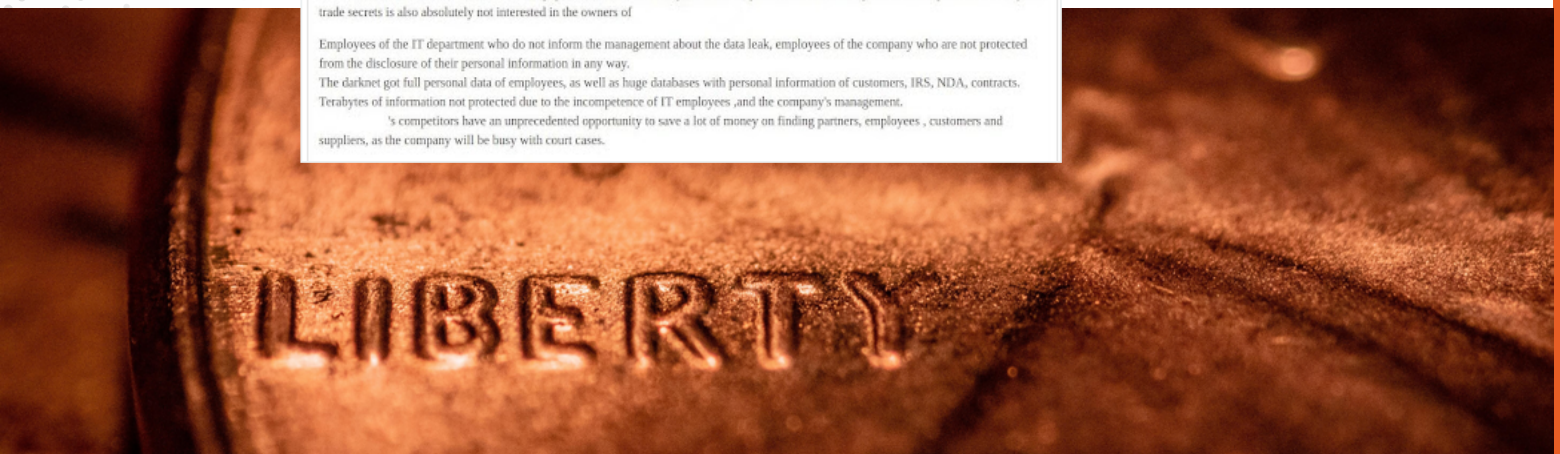
Unsightly details were revealed as a result of a powerful cyber attack on one of the largest producers of alcohol, . The revealed information contains exhaustive facts proving the company's irresponsible attitude to the personal data of customers, suppliers , partners and its own employees. And this is the company that calls itself the largest exporter of wines?

Lawyers of Coca Cola, Blue Apron Inc., P&L Specialties, Paquette Electic Company Inc, American Recycling Company LLC ,AutoCoding Systems LLC. Constellation Brands US Operations, Inc., Blackburn Consulting, VN Graphics, Inc., Czap Research and Development LLC, Deerland Enzymes, Inc., De La Rue Authentication Solutions, Inc., Exponent, Inc., SPS Commerce, Inc., Jordan Creative, LLC, Integrated Telecom Solutions, Inc., Collaborating Component Solutions C3, Inc., Royal Dutch Distillers. llc., National Distributind Company , Inc., Technicote, Inc. - and many other will definitely not be left without work in this difficult covid time. Nondisclosure agreement for costs no more than a blank sheet of paper. You should choose your business partners more carefully, because the preservation of your trade secrets is also absolutely not interested in the owners of

Employees of the IT department who do not inform the management about the data leak, employees of the company who are not protected from the disclosure of their personal information in any way.
The darknet got full personal data of employees, as well as huge databases with personal information of customers, IRS, NDA, contracts. Terabytes of information not protected due to the incompetence of IT employees ,and the company's management.
's competitors have an unprecedented opportunity to save a lot of money on finding partners, employees , customers and suppliers, as the company will be busy with court cases.

FIGURE 3

The REvil ransomware group highlights specific types of files in its data disclosure that it claims will severely damage the victim's business.



Data Disclosures as Indicators of General Ransomware Trends

Distribution of Incidents by Group and Time

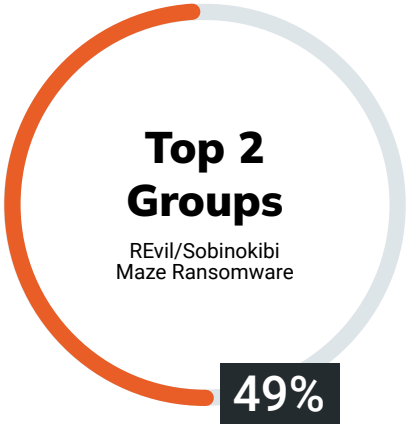
The now-defunct Maze ransomware group remained the leader of the double extortion tactic in 2020, accounting for 30% of all 94 reported April-December 2020 incidents. This huge "market share" is remarkable since Maze was active for only 10 out of 12 months that year before shutting down in early November 2020. That shutdown correlated to the decrease in reported incidents that month. The other top ransomware groups with data disclosures that year were REvil/Sodinokibi (19%), Conti (14%), and NetWalker (12%). It is worth highlighting that the top two groups of April-December 2020 alone accounted for nearly half (49%) of all reported 2020 incidents, and the top four groups alone accounted for three-quarters (75%) of all reported 2020 incidents. The ten other groups reported that year accounted for roughly the remaining quarter of all reported 2020 incidents.

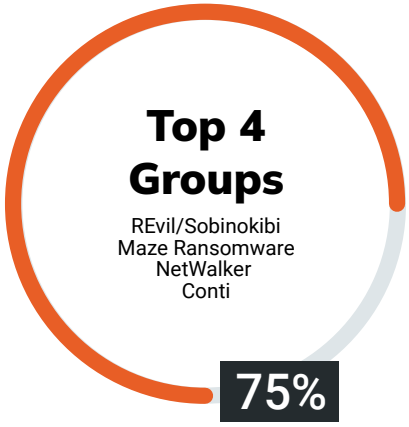
"

The now-defunct Maze ransomware group remained the leader of the double extortion tactic in 2020, accounting for 30% of all 94 reported April-December 2020 incidents.

FINDINGS

Top Ransomware Groups with Data Disclosures in 2020





30% Maze Ransomware

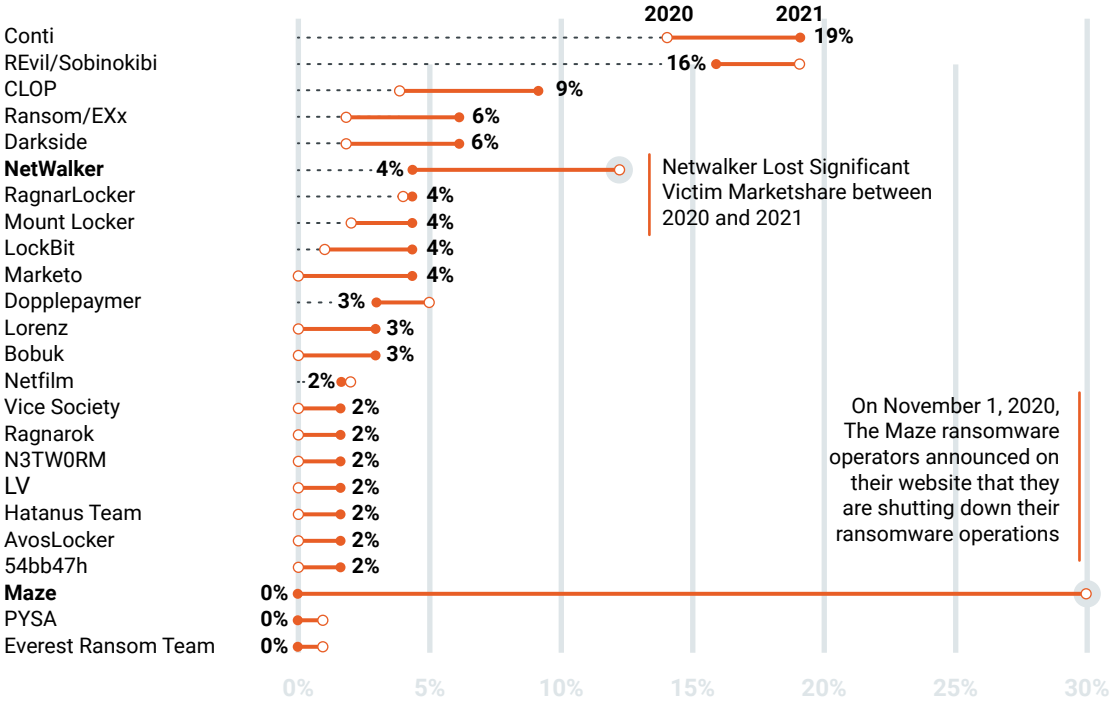
19% REvil/ Sobinokibi

14% Conti

12% NetWalker

25% Other

Ransomware attacks per attacker group over time.



Some groups fell off the map due to retirement or enforcement actors while others appeared on the scene to pick up victim marketshare

This concentration of a large proportion of activity in the hands of a relatively small number of groups decreased in 2021 with: a) the disappearance of Maze and: b) the entry into the market of a greater number of groups that each had smaller numbers of reported incidents. Conti (19%) and REvil/Sodinokibi (16%), which had been "runners-up" in the era of Maze, moved into the top positions, but with little change in their respective market shares. While Maze and REvil/Sodinokibi alone accounted for almost half of all observed activity as the top two groups in 2020, Conti and REvil/Sodinokibi alone accounted for just over one-third (35%) of all observed 2021 activity as the top two groups that year. CL0P increased its market share (9%) from the previous year to become the third most active group. Darkside and RansomEXX also increased their respective market shares from 2% to 6% each.

Beyond these top five groups, none of the other 16 groups with reported 2021 incidents were responsible for more than 5% of them. It took five of the top groups of 2021 to account for a majority 56% of reported 2021 incidents, whereas it only took the top two groups of 2020 to account for a near-majority of 2020 incidents. In other words, the demise of the historic market leader Maze created a vacuum that many less prolific groups tried to fill, resulting in more evenly distributed market share.

The demise of the historic market leader Maze created a vacuum that many less prolific groups tried to fill, resulting in more evenly distributed market share.

Identification and Distribution of Data Sets in Ransomware Data Disclosures

Analyzing the particular record types included in the data disclosures offers an opportunity to understand the overall prevalence of particular document types. In general, financial and accounting data was disclosed in the majority of double extortion incidents, followed by customer data and employee data. While these trends hold across our dataset, we find that the trends vary slightly by industry. Given the relatively small sample size for many industries, we focus in depth on verticals/sectors with either the largest number of incidents or with the most distinctive patterns: Financial Services, Healthcare, and Pharmaceuticals. Definitions of the 10 data categories are in the Appendix.

82%
of financial service data leaked were customer & patient information

50%
of the data disclosures were internal finance & accounting documents

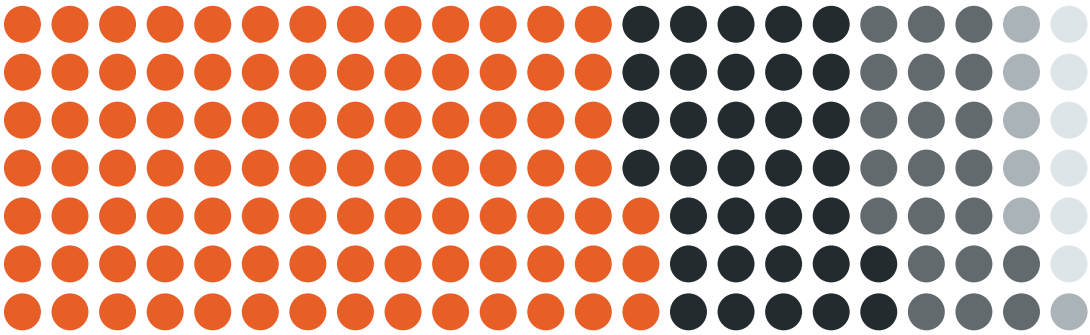
63%
of overall incidents across industries were finance & accounting documents

27%
of victims were vulnerable to future IT attacks

59%
of data came from Employee PII & HR

FINDINGS

Ransomware attacks by geographical region



North America
94 incidents (58%)

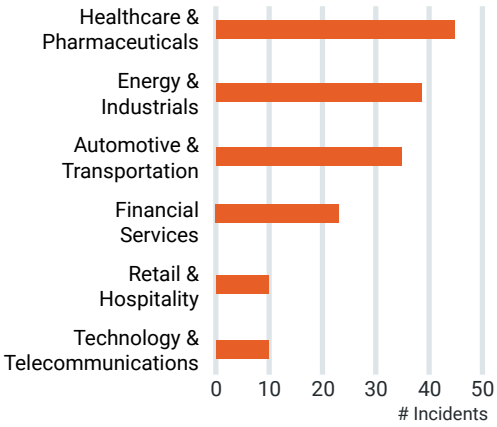
Europe
34 incidents (21%)

Asia-Pacific
21 incidents (13%)

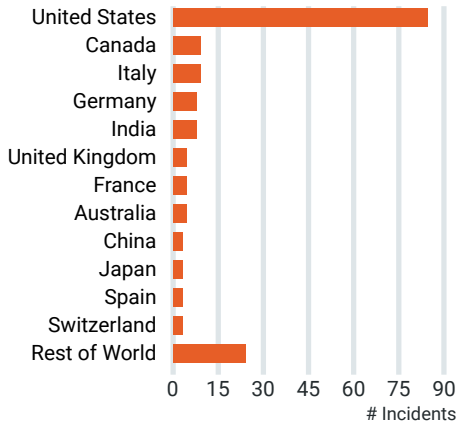
Middle East & Africa
6 incidents (4%)

Latin America
6 incidents (4%)

Distribution of Ransomware Incidents by industry



Distribution of Ransomware Incidents in Top 12 Countries



Trends by Industry

Financial Services

The most frequently observed category of files in any one industry, appearing in a remarkable 82% of disclosures from Financial Services victims (18 out of 22), was Customer & Patient data. The frequency with which the various categories of files appeared in data disclosures from Financial Services victims varied significantly from the total cross-industry sample. Internal Finance & Accounting documents, the most common category in the cross-industry sample, appeared in only 50% of the data disclosures from Financial Services victims (11 out of 22 incidents), compared with 63% of incidents overall. The data suggests that the ransomware attackers responsible for these disclosures chose to emphasize Customer & Patient data in order to undermine consumer trust in these organizations. The Financial Services industry is uniquely security-centric among private sector organizations and depends heavily on the perceived trustworthiness of financial institutions and their ability to protect customer data and funds.

The second-most frequently observed category of files in this industry was Employee PII & HR, which was observed in a high 59% of disclosures from victims (13 out of 22). The findings suggest that this greater emphasis on employee data aims to undermine the confidence of security-conscious Financial Services employees in their employers. Disclosures from Financial Services victims also had a somewhat higher (27%) frequency of Reconnaissance for Future IT Attacks (6 out of 22 incidents). We believe that Reconnaissance for Future IT Attacks on victims aim to exert more psychological pressure on victims and would also be of greater interest to other criminals, given criminals' high level of interest in the usually harder to penetrate targets in this industry.

Frequency of Observed File Categories in Disclosures from Observed Sectors

	All Sectors	Financial Services	Healthcare	Pharmaceutical
Operational Documents	14% (n=22)	14% (n=3)	5% (n=1)	14% (n=2)
Reconnaissance for Future Attacks	20% (n=32)	27% (n=6)	10% (n=2)	7% (n=2)
Sales & Marketing	36% (n=58)	23% (n=5)	19% (n=4)	14% (n=2)
Employee PII & HR	**41% (n=66)**	**59% (n=13)**	10% (n=2)	36% (n=5)
Customer & Patient Data	**41% (n=66)**	**82% (n=18)**	**66% (n=14)**	**43% (n=6)**
Finance & Accounting	**63% (n=101)**	**50% (n=11)**	**71% (n=15)**	**71% (n=10)**
Email Correspondence	12% (n=19)	14% (n=3)	14% (n=3)	
Insurance	4% (n=6)	14% (n=3)		
Intellectual Property	12% (n=19)			**43% (n=6)**
Legal, Governance & Compliance	9% (n=14)		10% (n=2)	

Note: Columns do not sum to 100% since certain record types can be counted across multiple categories.

Healthcare and Pharmaceuticals

Surprisingly, internal finance and accounting files appeared more frequently in Healthcare & Pharmaceuticals disclosures (71% of the time) than any other industry, including the Financial Services industry itself. Customer & Patient Data also appeared with high frequency (58% of the time, or 25 out of 43 incidents) in data disclosures, albeit with notably less frequency than Financial Services (82%). Many of the other categories of files appeared far less frequently than in the total cross-industry sample, suggesting a greater emphasis on those top two categories of files in particular.

The high frequency with which Customer & Patient Data appears in these disclosures suggest attackers aim to exert greater pressure on victims with: a) the more severe legal and regulatory consequences of patient data breaches for hospitals and other healthcare providers and; b) the greater utility of the more detailed and granular patient data sets to criminals for identity theft and other forms of fraud.

This reasoning becomes clearer when considering Healthcare and Pharmaceuticals separately instead of as a single vertical. Hospitals and other healthcare providers focus on serving patients, whereas Pharmaceutical companies focus on creating products. In contrast, disclosures from the Pharmaceutical sector had an unusually high frequency of Intellectual Property files (43%). Pharmaceutical companies depend heavily on large intellectual property investments and attackers seeking to place maximum pressure on victims in the Pharmaceuticals sector could find the threat of exposing such valuable Intellectual Property a useful way to coerce them into paying.

Trends by Threat Actor Groups

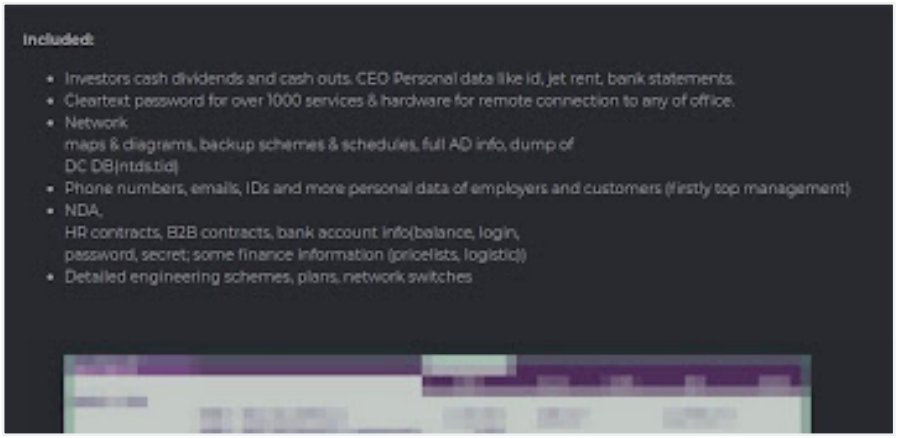
Some ransomware groups have a distinctive profile in the categories of files that they prefer to include in their disclosures. For example, the CL0P group has a markedly heavier emphasis on Employee PII & HR than the total sample of incidents across all groups. The prolific REvil/Sodinokibi group included Sales & Marketing files in its data disclosures with greater frequency than in the total sample across all groups. Conti's emphasis on the most popular category of files, Finance & Accounting, is markedly higher than that of the broader cross-group sample.

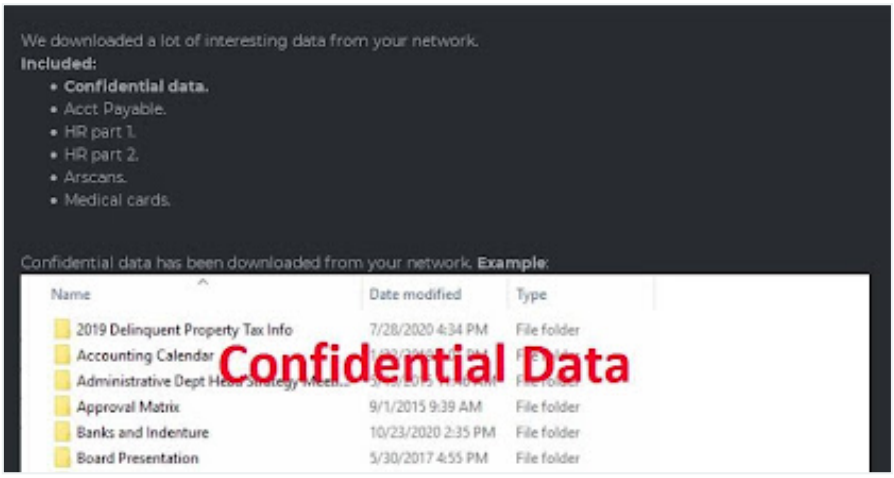
The former DarkSide group displayed the most distinctive "branding" for its data disclosures and had a more methodical approach to the packaging of its disclosures. DarkSide was responsible for the May 2021 attack on the Colonial pipeline. It later disappeared under that brand name, but the group or former elements thereof continued to operate under other brand names, including BlackMatter, BlackCat, and ALPHV. It prepared English-language summaries of data disclosure contents, written in higher-quality English than that of most other groups and with more extensive details about them.

Frequency of Observed File Categories in Disclosures from Observed Actors

	REvil	Cl0p	Conti	Darkside
Reconnaissance for Future attacks	28% (n=8)	20% (n=2)	4% (n=1)	33% (n=2)
Customer & Patient Data	**55% (n=16)**	30% (n=3)	**42% (n=11)**	**50% (n=3)**
Sales & Marketing	**48% (n=14)**	30% (n=3)	**46% (n=12)**	**67% (n=4)**
Employee PII & HR	**52% (n=15)**	**70% (n=7)**	27% (n=7)	**67% (n=4)**
Finance & Accounting	**55% (n=16)**	30% (n=3)	**81% (n=21)**	**100% (n=6)**
Email Correspondence	21% (n=6)		8% (n=2)	17% (n=1)
Insurance	3% (n=1)			17% (n=1)
Intellectual Property	10% (n=3)	20% (n=2)		
Legal Governance & Compliance	17% (n=5)		4% (n=1)	17% (n=1)
Operational Documents	17% (n=5)		12% (n=3)	17% (n=1)

Note: Columns do not sum to 100% since certain record types can be counted across multiple categories.



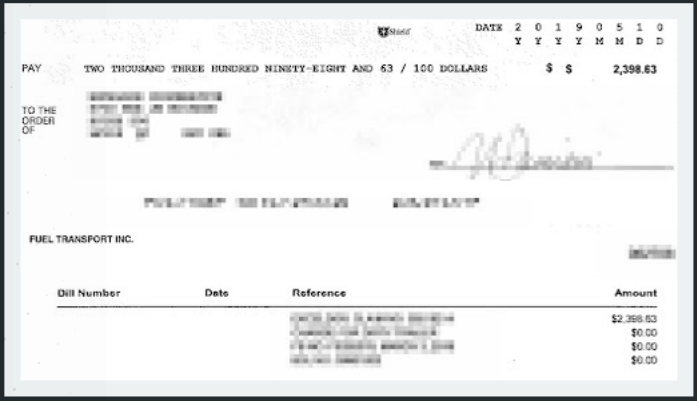


FIGURES 4 & 5

Examples of DarkSide's data disclosure summary messages.

DarkSide, operating under that brand name, was also more consistent than most other groups in its emphasis on the most popular categories of files. Our sample of DarkSide incidents was small but highlights this tighter consistency in that group's packaging of its disclosures. It was the only group to include one category of files (Finance & Accounting) in every single one of its multiple disclosures in our sample. It also displayed a more marked emphasis than the broader cross-group sample on the already popular categories of Employee PII & HR, Customer & Patient Data, Sales & Marketing, and Reconnaissance for Future IT Attacks, among others.

Examples of Files from Ransomware Data Disclosures



DATE 2019 05 10

PAY TWO THOUSAND THREE HUNDRED NINETY-EIGHT AND 63 / 100 DOLLARS $ $ 2,398.63

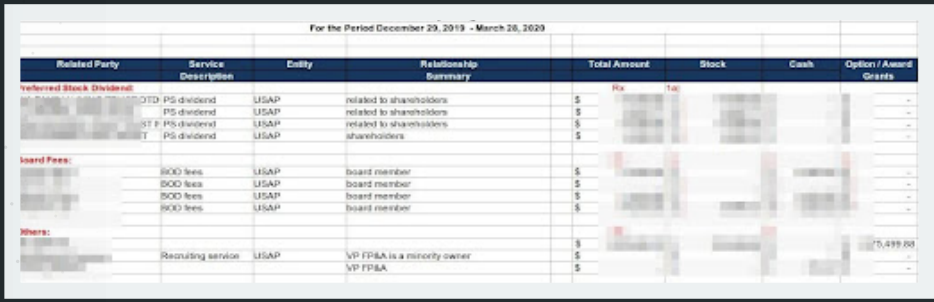
TO THE ORDER OF

FUEL TRANSPORT INC.

Bill Number	Date	Reference	Amount
			$2,398.63
			$0.00
			$0.00
			$0.00

FIGURE 5

A data disclosure includes copies of checks that a compromised company wrote.



For the Period December 29, 2019 - March 28, 2020

Related Party	Service Description	Entity	Relationship Summary	Total Amount	Stock	Cash	Option / Award Grants
Preferred Stock Dividend:							
OTD	PS dividend	USAP	related to shareholders	$			-
	PS dividend	USAP	related to shareholders	$			-
ST F	PS dividend	USAP	related to shareholders	$			-
T	PS dividend	USAP	shareholders	$			-
Board Fees:							
	BOD fees	USAP	board member	$			-
	BOD fees	USAP	board member	$			-
	BOD fees	USAP	board member	$			-
	BOD fees	USAP	board member	$			-
Others:							
				$			75,499.88
	Recruiting service	USAP	VP FP&A is a minority owner	$			-
			VP FP&A	$			-

FIGURE 6

A data disclosure reveals details on a compromised company's stocks.

Hello.

If you do not contact us, we will begin to publish your data.
Also on mails from your database we will send a link to this blog. Your customers will be happy to see their data in the public.

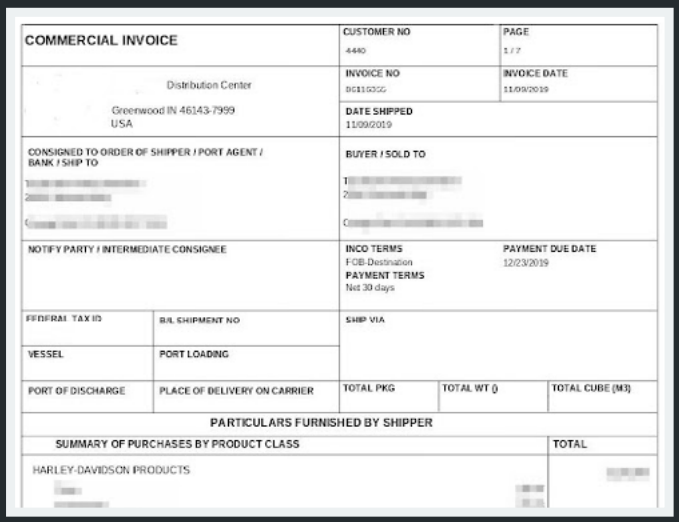
Some examples:

FIGURE 7

A ransomware group threatens to inform a compromised company's customers of the disclosure of their data via the compromise of that company

FIGURE 8

An invoice from a U.S. vehicle dealership.



COMMERCIAL INVOICE

CUSTOMER NO 4440 | PAGE 1 / 7

Distribution Center
Greenwood IN 46143-7999
USA

INVOICE NO [redacted] | INVOICE DATE 11/09/2019

DATE SHIPPED 11/09/2019

CONSIGNED TO ORDER OF SHIPPER / PORT AGENT / BANK / SHIP TO

BUYER / SOLD TO

NOTIFY PARTY / INTERMEDIATE CONSIGNEE

INCO TERMS FOB Destination
PAYMENT TERMS Net 30 days

PAYMENT DUE DATE 12/23/2019

FEDERAL TAX ID | B/L SHIPMENT NO | SHIP VIA

VESSEL | PORT LOADING

PORT OF DISCHARGE | PLACE OF DELIVERY ON CARRIER | TOTAL PKG | TOTAL WT () | TOTAL CUBE (M3)

PARTICULARS FURNISHED BY SHIPPER

SUMMARY OF PURCHASES BY PRODUCT CLASS | TOTAL

HARLEY-DAVIDSON PRODUCTS

CONCLUSION AND RECOMMENDATIONS

Ransomware attackers often choose their targets purposefully in the hopes of maximizing their profits and minimizing their risks and labor requirements. They are more likely to choose targets that they believe to be: more lucrative, easier to compromise, more likely to pay ransoms, and more suitable for short-term extortion than long-term data collection, based on the various types of data that they possess.

Ransomware attackers purposefully choose the types of data that they include in their data disclosures, in the hopes of maximizing the coercive impact of those disclosures on victims and on the basis of the damage that they can inflict. Internal financial records and customer and employee PII may be the most popular types of data selected for inclusion in data disclosures, but the selection of those files also varies by industry and by group. The sensitivity of each type of data varies by industry, and different groups may find certain types of data more sensitive than others.

This paper has not only substantiated the well-known preference of ransomware attackers for the Healthcare & Pharmaceuticals industry but has also revealed additional and occasionally unexpected nuances in the extensive targeting of that vertical.

Suggestions for responding to ransomware trends

Security professionals can put the contents of this report into practice in several ways.

- Organizations should construct lines of defense against both layers of double extortion ransomware attacks. Backups have long been the best line of defense against the file encryption layer, as they provide victims with an alternative to paying ransoms by giving them another way to restore their files.
- Backups, however, do not protect against the data disclosure layer of an attack. The best defenses against data disclosure include: file encryption, rendering any files unreadable to unauthorized eyes; and network segmentation, to reduce the likelihood that attackers will be able to move laterally to infrastructure housing key data assets, including backups.
- Organizations can use these findings to assess which specific data assets should receive additional protection, such as file encryption and network segmentation, based on the frequency with which they appear in relevant data disclosures.
- Organizations can use these findings to prepare for the event of a ransomware data disclosure if they anticipate what types of files are most likely to appear. For example, a bank or a hospital experiencing a ransomware incident should anticipate that any resulting data disclosure is likely to contain customer/patient data and take appropriate steps, such as preparing for customer/patient notifications. Most companies should also prepare for whatever adverse business consequences might result from the exposure of internal financial records.

Appendix: Definitions

Finance & Accounting: This category covers a company's internal finances and accounting. It includes files such as accounting records, balance sheets, company bank account details, checks, loan documentation, credit agreements, asset inventories, audits, budgets, tax records, financial statements, market capitalization documents, stock program details, and employee expense reports. The disclosure of these documents can damage a company in several ways, such as enabling financial fraud, creating legal or regulatory problems, or jeopardizing its reputation with investors and ability to acquire capital.

Customer & Patient Data: This category includes files about individual customers and patients that are not sales & marketing documents. It includes: personally identifiable information (PII) such as U.S. Social Security numbers (SSNs) or their equivalents in other countries; dates of birth (DOBs); copies of identity documents, such as drivers' licenses and passports; personal phone numbers; street and email addresses; digital copies of written signatures; credit reports and loan agreements; vehicle identification numbers (VINs); payment card or other billing details and billing statements; collections operations and insurance claims management; customer contact center records; credentials for customer-facing web portals or other online services; health insurance policy details; and medical records, including diagnoses, treatments, and imagery. These files damage a company's reputation by undermining consumer confidence in it, as these files enable multiple types of malicious activity against affected customers/patients such as identity theft and bank fraud.

Employee PII & HR: This category covers information about a compromised company's employees, including: PII, such as their U.S. SSNs or their equivalents in other countries, and DOBs; copies of identity documents, such as drivers' licenses and passports; personal phone numbers and street and email addresses; digital copies of fingerprints and written signatures; payroll files and W-2 tax forms; health insurance coverage and other benefits; performance reviews and personnel files; drug test results; job applications and recruiting; and resumes and training records. These files damage a company by exposing its employees to a variety of malicious activities and thereby undermining their trust in it and its ability to protect their information.

Sales & Marketing: This category covers files on a company's acquisition of customers and its provision of products or services to them. It includes documents such as order forms, invoices, receipts, contracts, purchase and non-disclosure agreements, sales techniques and policies, sales inquiries and leads, marketing strategies, and price lists. The disclosure of these documents harms a company by damaging its relationships with both actual and prospective customers and also by providing competitive intelligence to competitors.

Reconnaissance for Future IT Attacks: This category includes technical details that future attackers could use in another attack on the compromised company's information technology (IT). Employee directories and contact lists with work phone numbers and email addresses provide reconnaissance data for future attackers to use in phishing or other social engineering attacks. Compromised credentials provide initial access points. Lists of machines and maps of network architecture facilitate lateral movement. The details of a company's backup procedures can facilitate another ransomware attack, as ransomware attackers make a point of deleting or encrypting backups in order to deprive victims of an alternative to paying the ransom to restore their files.

Operational Documents: This category includes files detailing a company's business processes and procedures, as well as its operational technology (OT). Examples of this category include manuals, product inventories, health & safety procedures and reports, internal and inter-business codes, internal ticketing systems, facilities management, manufacturing procedures, engineering schematics, and utility network switches. The disclosure of this information can harm a company in multiple ways, including: enabling the manipulation of employees and business processes in a social engineering attack; facilitating an attack on a company's OT environment or Industrial Control Systems (ICS) with pre-attack reconnaissance; and exposing potential health & safety issues.

Intellectual Property: This category includes information on a company's proprietary products and services. Examples of this category, which vary significantly by industry and even by sector, include: source code for technology products and services or medical devices; formulas and descriptions for pharmaceutical products; exploration maps for oil & gas deposits; and engineering or manufacturing methods and schematics. This category may be qualitatively significant for some industries and sectors that depend heavily on intellectual property, but others may have little or no significant intellectual property at all. The disclosure of these files can harm a company by providing competitors with information with which to duplicate or outperform the compromised company's products and services, undermining the often significant investments that it made in that intellectual property. Future attackers could also use the source code of technology products and services to find security vulnerabilities in their products to exploit.

Email Correspondence: This category includes records of email communication among employees and between employees and customers, vendors, and other third-parties. These files can damage a company in multiple ways, such as by exposing competitive intelligence to competitors or revealing business practices that undermine its reputation or consumer confidence in it.

Legal, Governance, and Compliance: This category includes governance & compliance files and legal documents other than the sales contracts and non-disclosure agreements in the Sales & Marketing category. The disclosure of these documents can harm a company by exposing possible misconduct and by enabling criminals to tailor their attacks on the basis of a company's policies or its attorneys' legal opinions.

Insurance: This category includes documents detailing a company's insurance policies. The disclosure of these documents can damage a company by enabling criminals to tailor their attacks, particularly the amount of their ransom demands, on the basis of the victim's cyber insurance coverage.

POWER TO THE PROTECTORS

Our Philosophy

We believe that cybersecurity should be simpler and more accessible. Trusted by more than 9,300 customers worldwide, our best-in-class technology and strategic expertise draws on the insights of industry-leading researchers and contributions from the global security community to empower security professionals. The world has changed–Rapid7 is helping protectors be ready for what comes next.

PRODUCTS

insightCloudSec | insightIDR | Threat Command

insightVM | insightAppSec | insightConnect

To learn more or start a free trial, visit:
https://www.rapid7.com/try/insight/

SUPPORT

Customer Portal | Call +1.866.380.8113

RAPID7