# Capcom hit by Ragnar Locker ransomware, 1TB allegedly stolen

bleepingcomputer.com/news/security/japanese-game-dev-capcom-hit-by-cyberattack-business-impacted/

Lawrence Abrams

## By Lawrence Abrams

- November 5, 2020
- 11:05 AM
- 1



Japanese game developer Capcom has suffered a ransomware attack where threat actors claim to have stolen 1TB of sensitive data from their corporate networks in the US, Japan, and Canada.

Capcom is well-known for its iconic game franchises, including Street Fighter, Resident Evil, Devil May Cry, Monster Hunter, and Mega Man.

Yesterday, Capcom announced that they had been hit with a cyberattack on November 2nd, 2020, that led to the halting of portions of their corporate network to prevent the attack's spread.

"Beginning in the early morning hours of November 2, 2020 some of the Capcom Group networks experienced issues that affected access to certain systems, including email and file servers. The company has confirmed that this was due to unauthorized access carried out by a third party, and that it has halted some operations of its internal networks as of November 2."

Since the attack, Capcom has been displaying notices on its site warning visitors that emails and document requests will not be answered due to the attack impacting email systems.

#### Announcement

We are currently unable to reply to inquiries and/or to fulfill requests for documents via this form following the network issues that began November 2, 2020. Capcom deeply regrets any inconvenience this may cause. Please see the press release, "<u>Notice Regarding Network Issues due to Unauthorized Access</u>" for more details

## Notice about email being down

At the time, Capcom did not disclose the details of the cyberattack, but in a ransomware sample found by security researcher <u>Pancak3</u> we see that the Ragnar Locker ransomware gang attacked them.

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at <u>+16469613731</u> or on Wire at @lawrenceabrams-bc.

# Ransomware gang claims to have stolen 1 TB of files

After running the Ragnar Locker sample, we get access to the ransom note created on Capcom's computers during the attack. This ransom note provides a huge amount of visibility into the Ragnar Locker attack.

In the ransom note created during the attack, the Ragnar Locker operators state that they have stolen 1 TB of unencrypted files from the corporate networks in Japan, the USA, and Canada.

We have BREACHED your security perimeter and get access to every server of company's Network in different offices located in Japan, USA, Canada.

So we has DOWNLOADED more than 1TB total volume of your PRIVATE SENSITIVE Data, including:

-Accounting files, Banking Statements, Budget and Revenue files classified as Confidential, Tax Documents

-Intellectual Property, Proprietary Business information, Clients and Employees Personal information (Such as Passports and Visa), Incidents Acts

-Corporate Agreements and Contracts, Non-Disclosure Agreements, Confidential Agreements, Sales Summaries

-Also we have your Private Corporate Correspondence, Emails and Messanger Conversations, Marketing presentations, Audit reports and a lot of other Sensitive Information

If NO Deal made than all your Data will be Published and/or Sold through an auction to any third-parties

III.READ_ME_44027CDE_III.txt - Notepad2	- • ×
Eile Edit View Settings 2	
1**************************************	<u>^</u>
HELLO CAPCOM 1	
If you reading this message, it means your network was PENETRATED and all of your files and data has been ENCRYPTED	
7 by RAGNAR LOCKER! 8	
9 ************************************	
12 13 !!!!! WARNING !!!!! 14	
15 DO NOT Modify, rename, copy or move any files or you can DAMAGE them and decryption will be impossible. 16 DO NOT Use any third-party or public Decryption software, it also may DAMAGE files. 17 DO NOT Shutdown or Reset your system, it can DAMAGE files 18	E
19 20 There is ONLY ONE possible way to get back your files - contact us via LIVE CHAT and pay for the special DECRYPTION KEY 21 For your GUARANTEE we will decrypt 2 of your files FOR FREE, to show that it Works. 22	1
23 Don't waste your TIME, the link for contact us will be deleted if there is no contact made in closest time and you will DATA.	NEVER restore your
24 !!! HOWEVER if you will contact us within 2 day since get penetrated - you can get a very SPECIAL PRICE.	
26         ! WARNING !           27         ! Whole your International Corporate Network was fully COMPROMISED !	
28 29 We have BREACHED your security perimeter and get access to every server of company's Network in different offices local country of company's Network in different offices local	ated in Japan, USA,
Canada. 30 So we has DOWNLOADED more than 1TB total volume of your PRIVATE SENSITIVE Data, including: 31 -Accounting files, Banking Statements, Budget and Revenue files classified as Confidential, Tax Documents 32 -Intellectual Property, Proprietary Business information, Clients and Employees Personal information (Such as Passports Incidents Acts	and Visa),
<ul> <li>33 -Corporate Agreements and Contracts, Non-Disclosure Agreements, Confidential Agreements, Sales Summaries</li> <li>34 -Also we have your Private Corporate Correspondence, Emails and Messanger Conversations, Marketing presentations, Audit of other Sensitive Information</li> </ul>	reports and a lot
35 36 If NO Deal made than all your Data will be Published and/or Sold through an auction to any third-parties 37	
38	
<ul> <li>39 - There are some screenshots just as a proofs of what we got on you. (you can find more on Temporary Leak Page)</li> <li>40 Screenshots:</li> <li>41 https://prnt.sc//x////</li> <li>42 https://prnt.sc//x////</li> <li>43 https://prnt.sc//x///</li> </ul>	
44 https://prnt.sc/海豹海 45 https://prnt.sc/海豹海 46 https://prnt.sc/海豹海	
47 https://prnt.sc/ % %	-
Ln 59 : 86 Col 81 Sel 46 5.00 KB ANSI CR+LF INS Default Text	đ

## Capcom ransom note

Enclosed in the ransom note are seven print.sc URLs that display screenshots of stolen files, including employee termination agreements, Japanese passports, Steam sales reports from August, Bank statements, contractor agreements, and a screenshot of Active Directory Users and Computers MMC for the Capcom Windows domain.

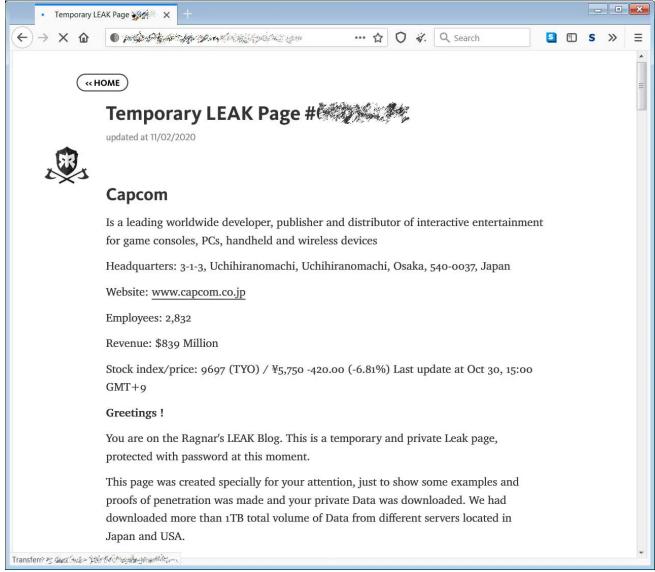
1	A	В	C	D	E	F	G	н		1	K
1	Steam Sales Report for Capcom: Augu	st 2020									
2	occant ourco report for capcorn. Augu	DC LOLO									
	Cales Denerty All state			-							
18	Sales Report: All platform	IS									
19	AVEA.	-	-		-	<b>•</b>	-	-	<b>•</b>	Revenue	
3	2010	Gross	Gross Units Sold	Chargeb acks/	Net Units Sold	Gross Steam Sales	Chargebacks/	VAT/Sales Tax	Net Steam Sales		US Share"US Share"US
20	Product (Id#)	Averag e Price	Gross Units Sold	Returns	Net Units Sold	Gross Steam Sales	Returns	Collected	Net Steam Sales	Total	Share-US Share-US Share-US Share-US Share-US Share-US
											StartUS Start
668	Street Fighter V - 2019 Summer Costume Bundle (360995)	28-90	1.58	11-11	14=5	\$12,200,19	182 23	(*622.97)	\$10.397,56	\$3,391.36	\$2,755.5
669	Street Fighter V - Mega Man Costume Bundle (360998)	af est	184	the state	16.1 st	S. Hinter	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	trank.	a touch	go allow the	Had 2
670	Street Fighter V - Summer 2019 Character Bundle (361004)	Arris 23	Sec. 34	13 fork	· lest in	Printing by the set	a 15.3.3 Mar	180.19 1003 1 Cal	the sound in the	4:5. No 4 40	100 1 64 14
671	Street Fighter V - M. Bison Costume Bundle / ベガコスチュームパック (30	El gots		£	172	7- 20	and the fit	14 3 4 14	1.391.20	the start	Willing the Mart
672	Street Fighter V - Zangief Costume Bundle (361010)	Erg. M.	4. 14	5 . 4	100 100	Section Ed.	109344	100 3	strayed.	4: Spartige	Acaste
673	Street Fighter V - Birdie Costume Bundle (361013)	1.4.2.45	43	177.4	33	Statering	Mar 19	Entry alle	1. Star 44 1	" for Set 183.	1. Optim
674	Street Fighter V - Vega Costume Bundle / パルログコスチュームパック (3)	12 3	and the second se	1 4	E.	Me Sa	Paster :	ant and	MORT	3 Dillar	1 That
	Street Fighter V - Rashid Costume Bundle (361019)	nests Ma	a part and the	1	and the	1 160.44	Condo.	Sugar Pris	in stan s	All de it it	Heaterlay
676	Street Fighter V - Dhalsim Costume Bundle (361022)	A. 16 3 4		4	#9	Apertin tin	Sand Trive	1+23/ B. J.	AUGAT	42.35	11. 30
677	Street Fighter V - F.A.N.G Costume Bundle (361025)	45. 20	10000	1 14	1100	Reyer	Set to THE	L'in at	at light in	242.55	the contract
678	Street Fighter V - Extra Battle CAPCOM LEGEND Bundle 2 (378381)	Minute State	14		100	122556 1964	Balart's	A start and	52. 2007	2.21.31.91	A. 3944
679	Street Fighter V - 2018 Halloween Costume Bundle (378384)	15.75	int	2 28.	4.7	Post Star Title	100 M. 13 8 14	filled at	St. Planty	3. M. G. DL	W. Site
680	Street Fighter V - Champion Edition Upgrade Kit (391974)	Est. a.	Burn's	12	1 the star	Standy M.	Same Section	Child and all all	Aright da	Ser. 4 2. 2 %	1 3 4 4 A 18 -
681	Street Fighter V - 2018 Holiday Costume Bundle (391977)	44	1545	1.91	18.50	1 hands	1200000	C'enon was	1.9 . 1	12.500.45	with the first
682	Street Fighter V - Extra Battle CAPCOM LEGEND Bundle 3 (391980)	. Heath	45	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	K. 6	min after to	Alg. Mi	Aller B.	2.1. km 16	100 15 and	sport is
683	Street Fighter V - Season 4 Character Pass (391986)	3 Sucher	100	54	2.127	124 × 6 41	the state of a	the the the	All Shape	series respects	5 5 Mar 31 45
	Street Fighter V - Champion Edition Special Color (no cost) (391989	- 2.12	91. B. O.		intral intral	the state of the state of the	ALL ALL A	the same a free way	and the second property of		an a standard and a standard and a standard a
	Street Fighter V - Champion Edition Special Wallpapers (no cost) (40*		here an	1. 18	Selling.	4	a an	and a free of the	se con many s	Contraction in Station	response interesting
	Street Fighter V - Capcom Pro Tour: 2020 Premier Pass (427624)	- Stalle	1.20	ing	15.7	Loty & plant	the thematica	1 to a for the for	lips were very	152.25.36	her the is
	Street Fighter V (432709)	1/4/141	the fairs	2 Sala	120.13	A Tradit of the	increased and a second	The got a start	a the second	and the los	Ser Sheet
	Phoenix Wright: Ace Attorney Original Soundtrack / 逆転散判サウンドBC	dige. 4	and a superior			gradite.	ne lation	and the second	d Astop rie	See. E.	11 1.10
	Phoenix Wright: Ace Attorney - Justice for All Original Soundtrack / #	distant.	10	4 . when	and the second second	A love to	17444	15 St 14	1. Sec. 25	in the	1 horalings
	Phoenix Wright: Ace Attorney - Trials and Tribulations Original Soun		and a second for	75 30 3	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	2 Burner	The Faller	1 - 1 - 1 - 19 F. F. B.	No alka ?	in intertain	140.78%
	Street Fighter V (310950): In-game Sales	6405	Seepers	34-134-14	1. Marchard	The for signation	NO MORE	a national	La stand all in	and ander	1. Company
	Ultra Street Fighter IV (45760): Community Market Game Fee		and the second sec	1 - Charles	Vinfar	and the second second	21-2-2-2-1- C-14	10 10 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Lade he	1 and and a	a sur
	SATAZIUS (203990): Community Market Game Fee		177 7.18	Dec.	the second second	1640	par average for the for	Concerning and the second	5	and and	s-un thinks
	eXceed - Gun Bullet Children (207370): Community Market Game Fe	16.4.14	See. 6	- 10-p	1 1 1 1	service it	100 mg	a series and a series and	14 154	1	insta
	eXceed 2nd - Vampire REX (207380): Community Market Game Fee	- Aught	1. S. 1.	and the second	and the states	2 Alar	1 18.2.0	Same and the second	12 B 1	1 68.15	tig light
	eXceed 3rd - Jade Penetrate Black Package (207400): Community M	and the	in the second	1	1.51 . 500	without our	Sold - Contraction	O'C BU AND	Arrah Shi	× 116 . 20	W1.9.6
	Street Fighter X Tekken (209120): Community Market Game Fee	the sec	anti-	124	in alters	19974	1.1.1	The share	1. 19 - 5 - 18 - 18 - 1 - 18 - 1 - 18 - 1 - 18 - 1 - 1	11 65. 900	1. 8. 2
	Ether Vapor Remaster (214570): Community Market Game Fee	- see the second		11/2010/00/	Color and the state	(By y size	- and the second second	the first and the second second	A 14-197	3 354 44	14 Y
	Fairy Bloom Freesia (214590): Community Market Game Fee	merer.	N. M. Berta	S. See	1.2.2.24		Sis. Yes	Sale and and and	Section 1	and!	the state of
	Cherry Tree High Comedy Club (214610): Community Market Game	Same.	4	E ALCONTRACTOR	110.00	en alice	and the second	2. ACT 55	1 tree and	alusta en	400 M.G
	DuckTales Remastered (237630): Community Market Game Fee	a starte	San Marine	Sector Contraction of the	37, 742	A. &	to the second	Antonia Carto In	the stand	18 18 Mer	Sugar
	Street Fighter V (310950): Community Market Game Fee	18	and the second s			and and the	- J- 21 - 2 4 5 9 2 4	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	Sales ardy	1. Anternation	\$9.341.40
	Mega Man Legacy Collection (363440): Community Market Game Feb		1 yes . 12		in the second	Section of	12 12 21-	The Phase	1. Actor in	Beach Sugar	and a second state
	Dragon's Dogma: Dark Arisen (367500): Community Market Game P		1943 50	1011 - 3	1 depint	abread when	1	The second in	the Big the	Step 5 40	in North
	Dead Rising (427190): Community Market Game Fee	- Alle	All Marshare	3 C 12	Sec. 10	A March		State State of	43 9245 76	2 3.60%-	Patrices
	The Disney Afternoon Collection (525040): Community Market Game	di the	12 11 14	San Charles	5 inc.	Section 1	時代の意義が行	2 Martin Charles	Aller St.	Sector Stands	de la compañía de la
	Dead Rising 4 (543460): Community Market Game Fee	18 2.				2 Solid to		The second	tony de	to meet the	See. 4
	Onimusha: Warlords (761600): Community Market Game Fee	16.00	Printer		100	FT AND	The states	The Crew	- THE SPACE	See da.	ALA
	Phoenix Wright: Ace Attorney Trilogy (787480): Community Market *	magazi		4.0-17.18	- 11 - 12 - 14 - 14 - 14 - 14 - 14 - 14	2 110 10 2 40.00	a company and	I starting the second	A CALLER	64 1.1	ine la
	Capcom Beat 'Em Up Bundle (885150): Community Market Game Fet	Elas	3.00	BUTTE IN T	and the second se		and a line of the	E TAN A AND AND	5-14 to	an Be	1
	Monster Hunter: World (582010): 5% Bonus Revenue Share	- T. 1846	1 1 2 2	AL AL	Water, the other of	Con 18 1 199 1 199 1	Carpel and and	depiction and the second	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	2 B. B. S. S.	The bar
712	the second	stoke 7 m	-1 Tool I share the	Fire f	Marthan Barbar	and the state	Sie Contractor	indian trinsfel	Man Martin	4 11 11 12 12	The contract
713			Real	Sunda Kina Bard	an and	taking Par. 134	the second of the	and a free free	A. 130.5.43	N	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1
714		-									
(14)											

## Stolen Capcom August 2020 Steam sales report

Redacted by BleepingComputer

Also enclosed in the ransom note is a link to a private data leak page on Ragnar Locker's website containing a 24MB archive containing additional stolen documents,

including revenue forecasts, salary spreadsheets, NDAs, immigration forms, corporate communications, and royalty reports.



## Capcom temporary data leak page

The ransom note contains a link to the Ragnar Locker Tor negotiation site, where Capcom can discuss the ransom demand with the attackers. At this time, the chat page has not been used by Capcom, so there is no indication as to the ransom amount Ragnar Locker is demanding.

Pancak3 told BleepingComputer tonight that Ragnar Locker claims to have encrypted 2,000 devices on Capcom's networks and are demanding \$11,000,000 in bitcoins for a decryptor.

This ransom also includes a promise to delete any stolen data and a network penetration security report.

It should be noted that ransomware negotiation service <u>Coveware</u> has seen ransomware operations increasingly <u>not keeping their promise to delete stolen data</u> after a ransom is paid.

Ragnar Locker has been involved in other massive attacks this year, including ones on Portuguese multinational energy giant Energias de Portugal (EDP), where a <u>\$10.9M</u> <u>ransom was demanded</u>. In September, they hit French maritime transport and logistics company CMA CGM, which <u>led to significant downtime</u> for the network and operations.

BleepingComputer has attempted to contact Capcom but has not received a response due to their email issues.

Update 11/5/20 7:00 PM EST: Added information on ransom amount.

## **Related Articles:**

Costa Rica declares national emergency after Conti ransomware attacks

New Black Basta ransomware springs into action with a dozen breaches

American Dental Association hit by new Black Basta ransomware

Wind turbine firm Nordex hit by Conti ransomware attack

Hackers use Conti's leaked ransomware to attack Russian companies

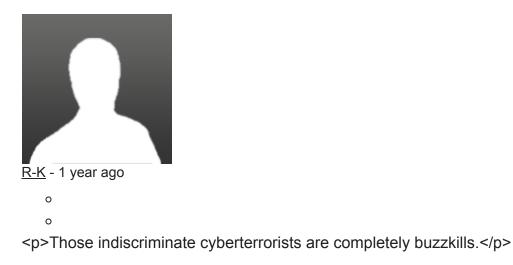
- <u>Capcom</u>
- <u>Cyberattack</u>
- <u>Games</u>
- Ragnar Locker
- Ransomware

## Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- <u>Next Article</u>

## Comments



Post a Comment <u>Community Rules</u> You need to login in order to post a comment Not a member yet? <u>Register Now</u>

You may also like: