

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, "[Notice Regarding Network Issues due to Unauthorized Access](#)" 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 [Pancak3](#) 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 [+16469613731](#) 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.

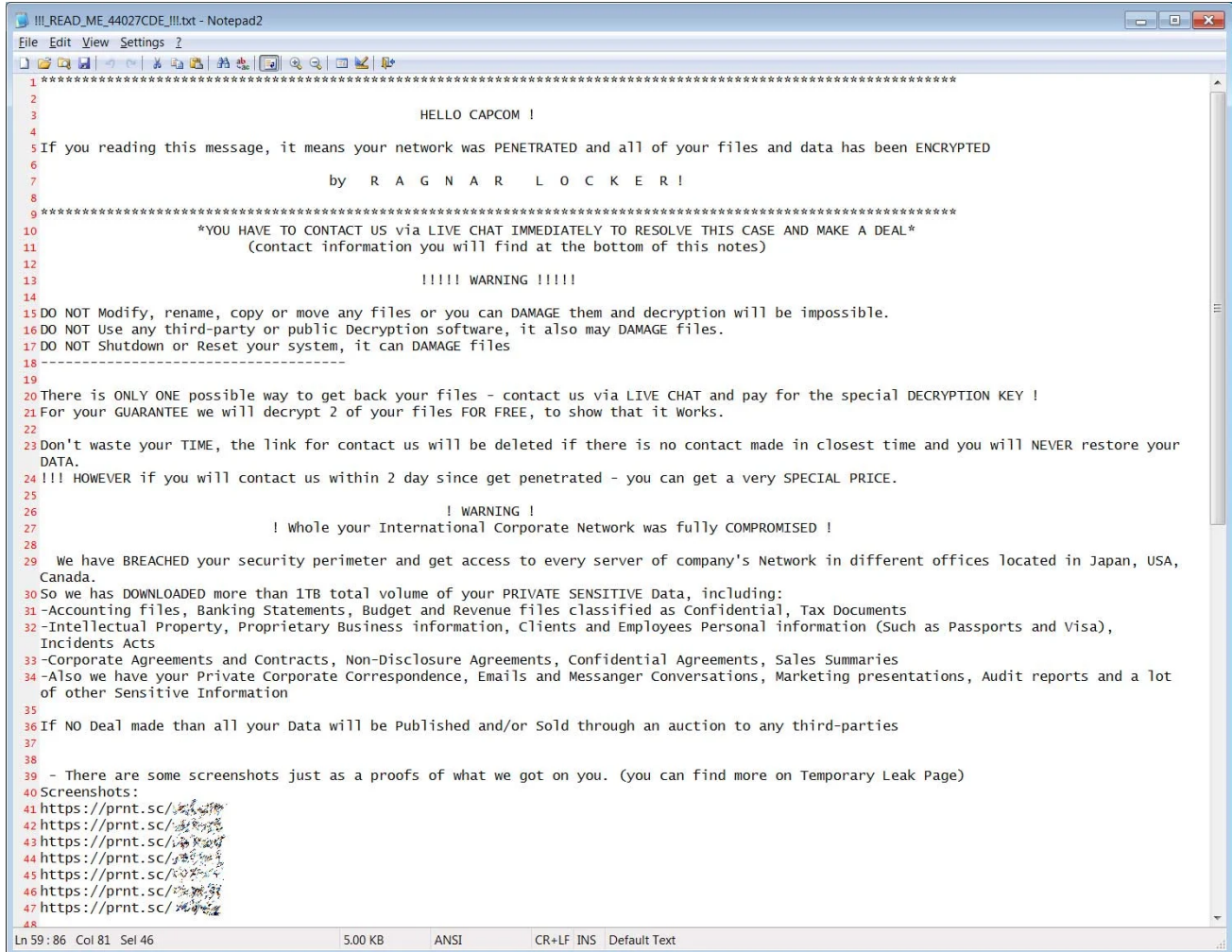
We have BREACHED your security perimeter and get access to every server of company's Network in different offices located in Japan, USA, Canada.

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 Messenger 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



```
!!!_READ_ME_44027CDE_!!!.txt - Notepad2
File Edit View Settings ?
*****
1
2
3
4 HELLO CAPCOM !
5 If you reading this message, it means your network was PENETRATED and all of your files and data has been ENCRYPTED
6
7
8 by R A G N A R L O C K E R !
9 *****
10 *YOU HAVE TO CONTACT US via LIVE CHAT IMMEDIATELY TO RESOLVE THIS CASE AND MAKE A DEAL*
11 (contact information you will find at the bottom of this notes)
12
13
14
15 !!!!! WARNING !!!!!
16
17 DO NOT Modify, rename, copy or move any files or you can DAMAGE them and decryption will be impossible.
18 DO NOT Use any third-party or public Decryption software, it also may DAMAGE files.
19 DO NOT Shutdown or Reset your system, it can DAMAGE files
20 -----
21 There is ONLY ONE possible way to get back your files - contact us via LIVE CHAT and pay for the special DECRYPTION KEY !
22 For your GUARANTEE we will decrypt 2 of your files FOR FREE, to show that it Works.
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 NEVER restore your
24 DATA.
25 !!! HOWEVER if you will contact us within 2 day since get penetrated - you can get a very SPECIAL PRICE.
26
27
28 ! WARNING !
29 ! Whole your International Corporate Network was fully COMPROMISED !
30
31 We have BREACHED your security perimeter and get access to every server of company's Network in different offices located in Japan, USA,
32 Canada.
33 So we has DOWNLOADED more than 1TB total volume of your PRIVATE SENSITIVE Data, including:
34 -Accounting files, Banking Statements, Budget and Revenue files classified as Confidential, Tax Documents
35 -Intellectual Property, Proprietary Business information, Clients and Employees Personal information (Such as Passports and Visa),
36 Incidents Acts
37 -Corporate Agreements and Contracts, Non-Disclosure Agreements, Confidential Agreements, Sales Summaries
38 -Also we have your Private Corporate Correspondence, Emails and Messenger Conversations, Marketing presentations, Audit reports and a lot
39 of other Sensitive Information
40
41 If NO Deal made than all your Data will be Published and/or Sold through an auction to any third-parties
42
43
44 - There are some screenshots just as a proofs of what we got on you. (you can find more on Temporary Leak Page)
45 Screenshots:
46 https://prnt.sc/...
47 https://prnt.sc/...
48 https://prnt.sc/...
49 https://prnt.sc/...
50 https://prnt.sc/...
51 https://prnt.sc/...
52 https://prnt.sc/...
Ln 59 : 86 Col 81 Sel 46 5.00 KB ANSI CR+LF INS Default Text
```

Capcom ransom note

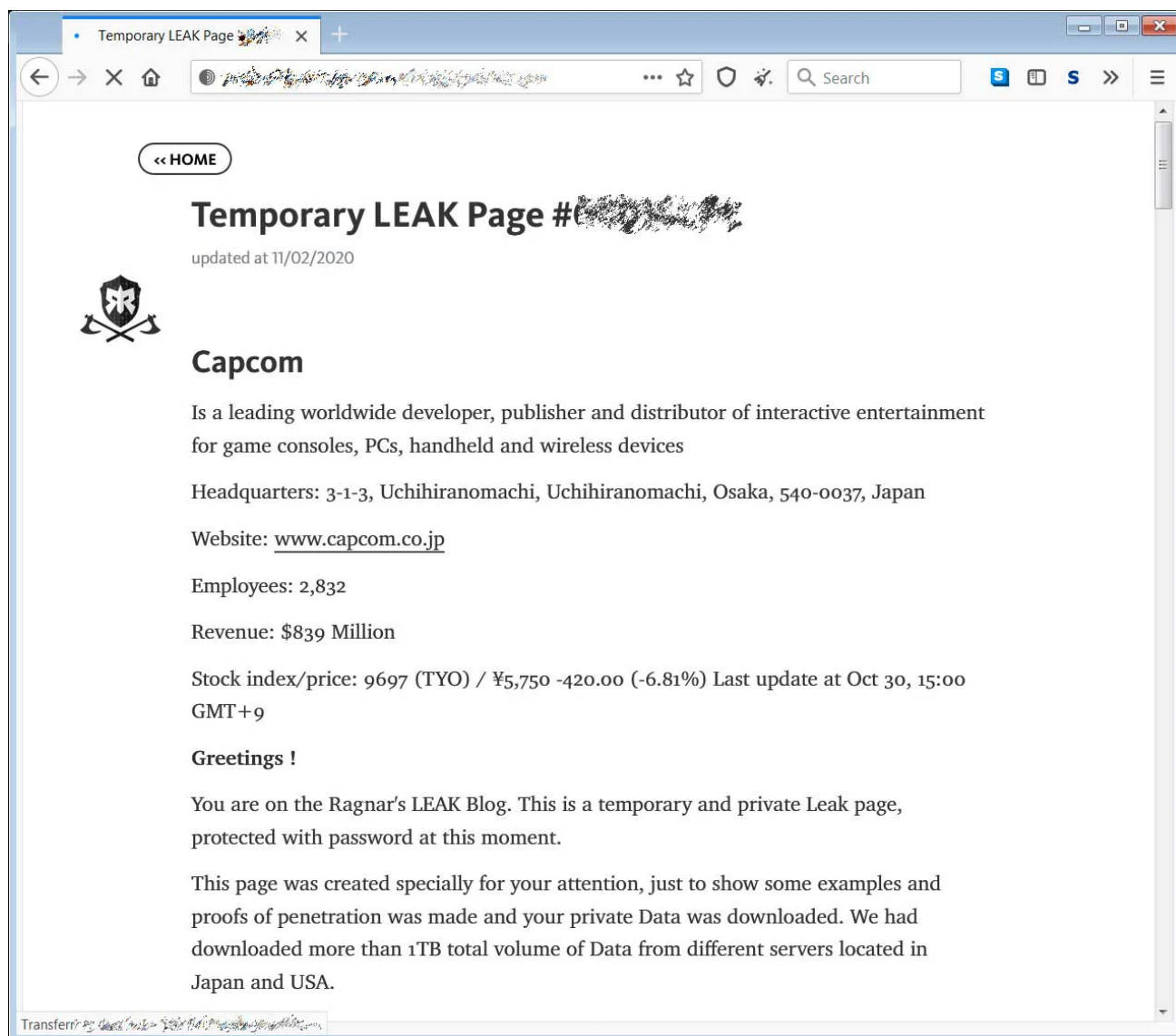
Enclosed in the ransom note are seven print.sc URLs that display screenshots of stolen files, including employee termination agreements, Japanese passports, Steam sales reports from August, Bank statements, contractor agreements, and a screenshot of Active Directory Users and Computers MMC for the Capcom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

Product (Id#)	Gross Average Price	Gross Units Sold	Chargebacks/Returns	Net Units Sold	Gross Steam Sales	Chargebacks/Returns	VAT/Sales Tax Collected	Net Steam Sales	Total	Revenue Share	US Share
668 Street Fighter V - 2019 Summer Costume Bundle (360995)											
669 Street Fighter V - Mega Man Costume Bundle (360998)											
670 Street Fighter V - Summer 2019 Character Bundle (361004)											
671 Street Fighter V - M. Bison Costume Bundle / ベガコスチュームパック (361004)											
672 Street Fighter V - Zangief Costume Bundle (361010)											
673 Street Fighter V - Birdie Costume Bundle (361013)											
674 Street Fighter V - Vega Costume Bundle / ベガコスチュームパック (361013)											
675 Street Fighter V - Rashid Costume Bundle (361019)											
676 Street Fighter V - Dhalsim Costume Bundle (361022)											
677 Street Fighter V - F.A.N.G Costume Bundle (361025)											
678 Street Fighter V - Extra Battle CAPCOM LEGEND Bundle 2 (378381)											
679 Street Fighter V - 2018 Halloween Costume Bundle (378384)											
680 Street Fighter V - Champion Edition Upgrade Kit (391974)											
681 Street Fighter V - 2018 Holiday Costume Bundle (391977)											
682 Street Fighter V - Extra Battle CAPCOM LEGEND Bundle 3 (391980)											
683 Street Fighter V - Season 4 Character Pass (391986)											
684 Street Fighter V - Champion Edition Special Color (no cost) (391989)											
685 Street Fighter V - Champion Edition Special Wallpapers (no cost) (401992)											
686 Street Fighter V - Capcom Pro Tour: 2020 Premier Pass (427624)											
687 Street Fighter V (432209)											
688 Phoenix Wright: Ace Attorney Original Soundtrack / 成歩堂かばんのサウンドトラック											
689 Phoenix Wright: Ace Attorney - Justice for All Original Soundtrack / 成歩堂かばんのサウンドトラック											
690 Phoenix Wright: Ace Attorney - Trials and Tribulations Original Soundtrack / 成歩堂かばんのサウンドトラック											
691 Street Fighter V (310950): In-game Sales											
692 Ultra Street Fighter IV (49760): Community Market Game Fee											
693 SATAZIUS (203990): Community Market Game Fee											
694 aXceed - Gun Bullet Children (207370): Community Market Game Fee											
695 aXceed 2nd - Vampire REX (207380): Community Market Game Fee											
696 aXceed 3rd - Jade Penetrate Black Package (207400): Community Market Game Fee											
697 Street Fighter X Takkan (209120): Community Market Game Fee											
698 Ether Vapor Remaster (214570): Community Market Game Fee											
699 Fairy Bloom Freesia (214590): Community Market Game Fee											
700 Cherry Tree High Comedy Club (214610): Community Market Game Fee											
701 DuckTales Remastered (237630): Community Market Game Fee											
702 Street Fighter V (310950): Community Market Game Fee											
703 Mega Man Legacy Collection (363440): Community Market Game Fee											
704 Dragon's Dogma: Dark Arisen (367500): Community Market Game Fee											
705 Dead Rising (427190): Community Market Game Fee											
706 The Disney Afternoon Collection (525040): Community Market Game Fee											
707 Dead Rising 4 (543460): Community Market Game Fee											
708 Daimonsha: Warlords (761600): Community Market Game Fee											
709 Phoenix Wright: Ace Attorney Trilogy (881480): Community Market Game Fee											
710 Capcom Beat 'Em Up Bundle (885150): Community Market Game Fee											
711 Monster Hunter: World (982010): 5% Bonus Revenue Share											
712											
713											
714											

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 Coveware has seen ransomware operations increasingly not keeping their promise to delete stolen data 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 [\\$10.9M ransom was demanded](#). In September, they hit French maritime transport and logistics company CMA CGM, which [led to significant downtime](#) 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](#)

- [Capcom](#)
- [Cyberattack](#)
- [Games](#)
- [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](#)
- [Next Article](#)

Comments



R-K - 1 year ago

-
-

<p>Those indiscriminate cyberterrorists are completely buzzkills.</p>

Post a Comment [Community Rules](#)

You need to login in order to post a comment

Not a member yet? [Register Now](#)

You may also like:
