FLASHPOINT

Intelligence Report

Cognizant Ransomware Incident

April 23, 2020

INCIDENT SUMMARY

On April 16, the "Maze" ransomware group successfully deployed ransomware against IT services firm Cognizant (cognizant[.]com). On April 18, posts on social media revealed that Cognizant was responding to a ransomware infection on their systems. Cognizant sent a notice to its customers that the "attack was limited to Cognizant's VDI environment and there was no client impact identified" as of April 18.

On April 19, the company publicly confirmed that "a security incident involving our internal systems, and causing service disruptions for some of our clients, is the result of a Maze ransomware attack." Flashpoint's Maze Analyst Knowledge Page details additional information on the past activities of the extortionist group.

It is unknown whether the Maze group was successful in exfiltrating information from the Cognizant network prior to deploying the ransomware. This group is notorious for stealing data before encrypting victims' devices and then issuing threats of publishing stolen data to coerce the victims to pay the ransom. Flashpoint maintains collections on the Maze website where stolen data is posted.

OVERVIEW OF MAZE GROUP

[Back to top]

The "Maze" ransomware family is based on the previous "ChaCha" ransomware. It utilizes RSA-2048 and ChaCha20 encryption. The ransomware note with instructions for payment is created under the distinct name "DECRYPT-FILES.txt." The note also refers victims to a public support site with an online chat service for further help.

Maze became a pioneer in new extortion tactics in which threat actors steal data prior to their encryption and then threaten publication if the ransom is not received on time. Some cybercriminals have tried to use these tactics in the past, but the Maze gang was the first to follow up on its threats, conducting an elaborate scheme of gradual data publication to show the seriousness of their intent.

Flashpoint analysts continue to track the actors behind Maze ransomware and follow their advertisement campaign on the Deep and Dark Web (DDW). Updates will continue to be published. For additional information regarding Maze and its victims, refer to the Maze Analyst Knowledge Page.

VICTIM ORGANIZATION: COGNIZANT

[Back to top]

According to the company, Cognizant is one of the world's leading professional services companies, transforming clients' business, operating, and technology models for the digital era.
Their services include digital services and solutions, consulting, application development, systems integration, application testing, application maintenance, infrastructure services, and business process services.

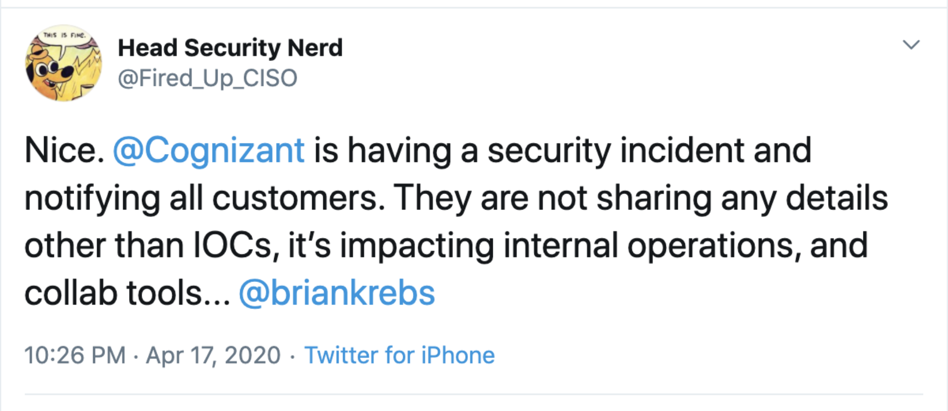
Business segments include financial services; healthcare; retail and consumer goods; manufacturing, logistics, energy, and utilities; and communication, media, and technology.

Cognizant is part of the NASDAQ-100 and trades under CTSH.

TIMELINE OF EVENTS

[Back to top]

- April 16, 2020: Maze ransomware is deployed on the Cognizant network.
- April 18: Cognizant notifies customers of incident.
    - 10:26 PM ET: Twitter user @Fired_Up_CISO reveals ongoing incident at Cognizant. (hxxps://twitter[.]com/Fired_Up_CISO/status/1251336338722480130)



Head Security Nerd
@Fired_Up_CISO

Nice. @Cognizant is having a security incident and notifying all customers. They are not sharing any details other than IOCs, it's impacting internal operations, and collab tools... @briankrebs

10:26 PM · Apr 17, 2020 · Twitter for iPhone

Image 1: Tweet from account @Fired_Up_CISO reporting the Cognizant incident.

- April 19: The Cognizant Security Incident Update blog publicly acknowledges the Maze ransomware incident. The full update from Cognizant (source: hxxps://news[.]cognizant[.]com/2020-04-18-cognizant-security-update):

> *Cognizant can confirm that a security incident involving our internal systems, and causing service disruptions for some of our clients, is the result of a Maze ransomware attack.*
>
> *Our internal security teams, supplemented by leading cyber defense firms, are actively taking steps to contain this incident. Cognizant has also engaged with the appropriate law enforcement authorities.*
>
> *We are in ongoing communication with our clients and have provided them with Indicators of Compromise (IOCs) and other technical information of a defensive nature.*

INDICATORS OF COMPROMISE

[Back to top]

Known technical indicators from this incident can be found here in CSV format, here in MISP JSON, and here in the Flashpoint API.

April 18, 2020

MD5	SHA256	Filename
910aa49813ee4cc7e4fa0074db5e454a	4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a	kepstl32.dll
76f8f28bd51efa03ab992fdb050c8382	5470f0644589685000154cb7d3f60280acb16e39ca961cce2c016078b303bc1b	memes.tmp
b6786f141148925010122819047d1882	c84b2c7ec20dd835ece13d5ae42b30e02a9e67cc13c831ae81d85b49518387b9	maze.dll
11308e450b1f17954f531122a56fae3b	9845f553ae868cd3f8d8c3f8684d18f226de005ee6b52ad88b353228b788cf73	N/A

IP Addresses
91[.]218[.]114[.]4
91[.]218[.]114[.]11
91[.]218[.]114[.]25
91[.]218[.]114[.]26
91[.]218[.]114[.]31
91[.]218[.]114[.]32
91[.]218[.]114[.]37
91[.]218[.]114[.]38
91[.]218[.]114[.]77
91[.]218[.]114[.]79

April 22, 2020

MD5	SHA256	Filename
7507fe19afbda652e9b2768c10ad639f	6d4836c75092d75f1d3a1d90100f19247473f9b0d7e12602221a7badf7feb29d	8e6ce49.exe
a93b86b2530cc988f801462ead702d84	e49225cc26ec911a213eb942d7797e8eec6de3f793abc8bb30f4b89f14e72d96	3686576.exe
4f57e35a89e257952c3809211bef78ea	b27bfa476a6915e573583c63b1d898913472ed86f224d5c470051359ceff8828	17269b5.exe
bad6fc87a98d1663be0df23aedaf1c62	f97bda917e52379ae9fe06605e4f120f9c88aebea38d3b4aeb3c21d476ea4d39	mrtscp64.exe
f5ef96251f183f7fc63205d8ebf30cbf	92125cc9aec53e2e7d0a67e8a53f0d6cb4a33f9ca73243d66b0397d7ddec907e	jarvey.exe
c818cc38f46c604f8576118f12fd0a63	3fd37d42d5821a8cbcf930255ca1259a680937e4e7dfa2d535d56121187806c2	KarriBillabong.dll
078cf6db38725c37030c79ef73519c0c	eed70e8b4425aea2c6cd37c06c8789acbc049269d6f56d8968787383e82d23dc	5f83030.exe
c255daaa8abfadc12c9ae8ae2d148b31	0606c6d918e0c02cea5fd85bfeb862c8ffe3eee4ef059cd8d2cd3ff342fdf9d9	4ffcc27.exe
1fef99f05bf5ae78a28d521612506057	94673f34efc32e73523f8435acf0afce782ba4f68e9f71f80afbeb3b917162f3	ac2c822.exe
cebe4799b6aff9cead533536b09fecd1	67f338c9f15b000aedac1d736fbce1ab27fd72a10d397315ba724b1dccf4e834	kinput.dll
f5ef96251f183f7fc63205d8ebf30cbf	92125cc9aec53e2e7d0a67e8a53f0d6cb4a33f9ca73243d66b0397d7ddec907e	jarvey.exe
bad6fc87a98d1663be0df23aedaf1c62	f97bda917e52379ae9fe06605e4f120f9c88aebea38d3b4aeb3c21d476ea4d39	mrtscp64.exe
910AA49813EE4CC7E4FA0074DB5E454A	4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a	kepstl32.dll
3A5A9D40D4592C344920DD082029B362	d215134b504790b3a3850e4e28a056a5eb2afdd057828626838507792476a74d	lckwmi.bat

FAD3C6914D798E29A3FD8E415F1608F4	abb36315ed6f708ba60c8cf70fdc0e327f7fbcfdfe33a403827e47a0155d1e4f	lckwmi.bat

IP Addresses
37[.]252[.]7[.]142
104[.]18[.]40[.]94

Domains
thesawmeinrew[.]net
drivers[.]updatecenter[.]icu
updates[.]updatecenter[.]icu

UNSUBSTANTIATED RESEARCH LEADS

[Back to top]

Research Lead #1: The UAS RDP underground market has several Remote Desktop Protocol (RDP) accesses for sale to Cognizant networks. Flashpoint is using its accesses within the shop to validate exposure.

Research Lead #2: Various researchers have questioned whether the April 6 post by Russian-speaking actor “SHERIFF” offering access to an IT support and services company is related to this incident (source: hxxps://twitter[.]com/underthebreach/status/1251605359409664005). At this time, there is no evidence that the two are connected, but the timing does raise several research leads. Flashpoint will continue to vet this claim. However, it is unlikely SHERIFF would reveal any details outside of their parties involved in the unverified transaction.

The original Flashpoint alert sharing this possibility on FPCollab is as follows.

> *Dear Team,*
>
> *On April 6, 2020, on Exploit, a top-tier Russian-language cybercrime and hacking forum, the notorious Russian-speaking actor “SHERIFF” offered access to an IT support and services company.*
>
> *This offer is noteworthy because of the high asking price, as well as an array of affected entities across various industries.*
>
> *According to the threat actor, the access includes sixty networks with approximately 1,200 PCs.*
>
> *The threat actor does not specify names of the clients of the affected company, however, they do list general information about each entity:*
>
> *- Access to a law firm. running a single server. The amount of data is 5 terabytes.*
> *- Swiss Bank*
> *- A large architectural firm, with 3 offices internationally (access to 55 PCs and 3 servers, 30 terabytes)*
> *- New York State Real Estate Brokerage, server access, 6 terabytes.*
> *- Access to a large construction firm (well-known multi-billion dollar objects, the largest one valued at 20 billion USD, access to 16 PCs, 1 server, 1.5 terabytes)*
> *- Scientific company (technology development, well-known customers, government orders. Access 80 PCs, Switch, Router, 2 servers, 11 terabytes)*
> *- The company working with news channels, events, design, equipment (a leader in its industry. Access to 15 PCs, router, 5 terabytes)*
> *- Financial consultancy (asset management, consultations, works with offshore companies, corporate clients. Access to 40 PCs, router, 4 servers, 1 terabyte)*
> *- "The largest event management agency in the country" (the country is not specified)*
> *- The company is the world's largest producer (in its field). Revenue is 5 billion USD, access to 90 PCs, router, 7 servers, 9 terabytes*
> *- Bank (Access to 15 PCs, Switch, Router, 2 servers, 2.5 terabytes)*
> *- Luxury hotel chain (Access to 80 PCs, 3 servers, 16 terabytes)*

- *Architecture, design firm, many famous clients (Access to 90 PC, Switch, Router, 5 servers, 25 terabytes)*
- *Architect firm (Access to13 PCs, 1 server, 16 terabytes)*
- *Real estate company (Access to 20 PCs, 3 servers, 8 terabytes)*
- *An international company in the field of broadcast media, marketing and sports (Access to 10 PCs, Switch, Router, 1 server, 3.5 terabytes)*
- *A telephone operator, very popular in the country (the TA is likely referring to the US) Access to 2 PCs, 40 servers, 65 terabytes (42T on the main server)*
- *Maritime company (Access to 15 pc, router, 2 servers, 600 GB)*
- *Access to a factory, the largest in Europe in its field. (2 servers, 4.6 terabytes)*
- *Real estate developing company (Access to 45 PCs, router, 2 servers, 5.7 terabytes)*
- *An international hospitality, real estate and tourism company (Access to 20 PCs, router, 1 server, 3 terabytes)*
- *International Tobacco Company (Access to 45 PCs, router, 3 servers, 5 terabytes)*
- *Advertising and marketing services company(1 billion USD in revenue, access to 2 PCs, router, server, 2 terabytes)*
- *Luxury resort (Access to 10 PCs, 2 servers, 2 terabytes)*
- *An interior decoration company leading in the country (likely the US), many orders from the government (Access to 60 PCs, 6 servers, 4 terabytes)*
- *Air company equipment supplier (Access to 12 PCs, router, 3 servers, 1.5 terabytes.*

The threat actor claims that access to each PC or server allows viewing the service controller information.

Additionally, the threat actor noted that the type of information differs with each access: User information, email data, hosts, VPN.

The threat actor also states that they chose "the most interesting companies;" according to the threat actor, there are other "smaller companies, as well as access to the servers of the IT company itself." Additionally, the TA noted that the revenue of the largest company from the above list is $18 billion USD. In order to connect, a new admin domain access will be created. According to SHERIFF, the access offered allows access to companies' VNC, RDP, Splashtop, the ability to view tickets, and control the routers.

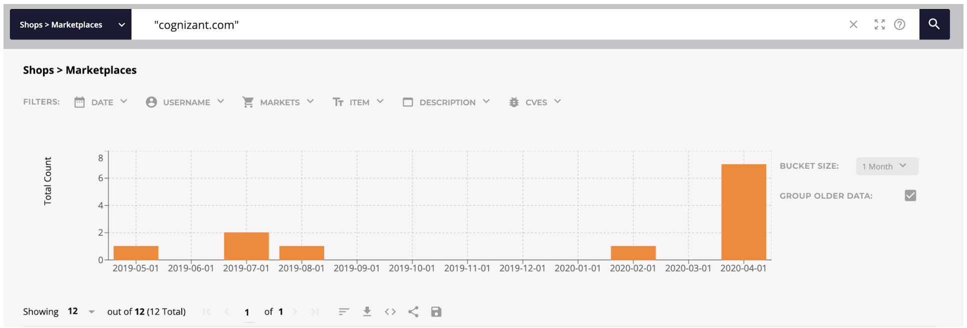
As of April 6, 2020, the starting price was set at $200,000, bids in increments of $50,000, and the buy-it-now price was not specified.

On April 10, 2020, the starting price was lowered down to $170,000. Additionally, the threat actor noted that he will not give out links to any companies.

On April 13, 2020, the starting price was lowered to $130,000.

Flashpoint analysts are continuing to closely monitor SHERIFF's activities and will provide updates as necessary.

Research Lead #3: Several Cognizant[.]com accounts have been offered on Genesis Market over the past several months. Flashpoint is reviewing current availability.



"cognizant.com"

Shops > Marketplaces

Showing 12 out of 12 (12 Total) 1 of 1

Note: This report previously mentioned a possible connection to "Snatch" ransomware but after further investigation by Flashpoint analysts, no connection can be made. The authors of the source of information and other researchers in the field have performed additional review and confirm that no connection can be established. It appeared that the Maze IoCs were added by mistake to the list of Snatch IoCs.

=======

All Flashpoint intelligence reports, related data, and content are the property of Flashpoint, and are protected under all applicable laws. Flashpoint reports and data are intended solely for the internal use of the individual and organization to which they are addressed, and are subject to the applicable terms and conditions of your Subscription Agreement with Flashpoint and/or your NDA, as applicable. Flashpoint reports and data are Flashpoint Confidential Information, and as such, may not be shared outside of your company or disclosed publicly for any purposes without Flashpoint's written consent; provided, however, that you may share such materials to third parties if legally required, or on a need-to-know basis, and then only to those parties who are bound by confidentiality obligations no less protective of Flashpoint than those contained in your Agreement and/or your NDA.

=======