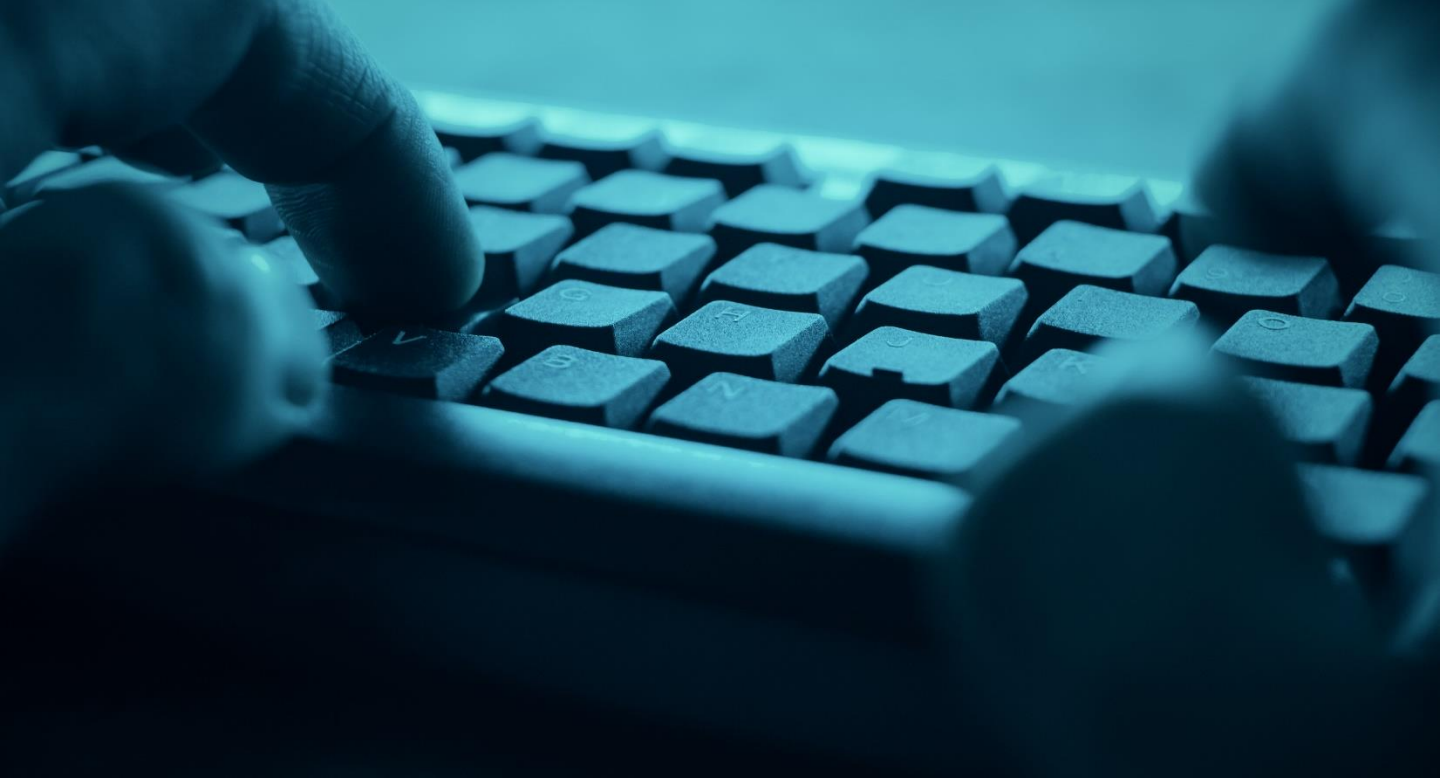
BDO'S CYBERSECURITY CENTER
CYBER THREAT INSIGHTS (CTI)

FOCUS ON:

GARMIN'S RANSOMWARE ATTACK

Summer 2020 Report



PREFACE

A large-scale ransomware attack crippled the GPS and aviation tech company, Garmin, somewhere around Thursday, July the 23rd. Garmin were infected by 'WastedLocker' Ransomware, which took down the company's systems and services.

WastedLocker which is operated by Russian cyber group called Evilcorp, disrupted Garmin's business operations and services for more than several days, before they were able to obtain the decryption keys.

Garmin allegedly paid the ransom, estimated to be around $10M USD. Since the average size of ransomware attacks in Q4 of 2019 was $111,605[1], and $780,000 for large enterprises[2], the amount in the case of Garmin, is exceptional.

Just to emphasis, the average total cost of a breach so far globally, in 2020 is around $3.86M USD ($3.9M at 2019) and $8.64M USD[3] in the USA only. Garmin's ransom payout is almost 13 times bigger than the averaged ransom for large enterprises and 2.5 times bigger than the total global average in 2020, that's before taking into consideration the downtime and its business implications.

> "AVERAGE TOTAL COST OF A CYBER-ATTACK IN 2020 IS $3.86 GLOBALLY AND $8.64 JUST IN THE U.S."

1 https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report

2 https://purplesec.us/resources/cyber-security-statistics/ransomware/

3 https://securityintelligence.com/posts/whats-new-2020-cost-of-a-data-breach-report/ ; https://www.ibm.com/security/digital-assets/cost-data-breach-report/?utm_medium=OSocial&utm_source=Blog&utm_content=000039JJ&utm_term=10013747&utm_id=SI-blog-1&cm_mmc=OSocial_Blog-_-Portfolio%20Security_Security%20Conversation-_-WW_WW-_-SI-blog-1_ov76748&cm_mmca1=000039JJ&cm_mmca2=10013747&_ga=2.99248856.752724313.1596694702-1773476305.1596694702#/

COMPARISON TO OTHER RANSOMWARE ATTACKS

The past year we came across other ransomware attacks, in which hackers demanded exceptional amounts of money. The first one is a ransomware attack from November 2019 on a Mexican oil company named Pemex. Hackers used the 'DoppelPaymer' to attack company's networks and encrypted sensitive data. They demanded $4.9M USD for decrypting back the data.[4] The second one from September 2019 was a ransom attack on New Bedford Municipality in Massachusetts. The hackers used 'Ryuk' ransomware and encrypted data on 158 computers. Ransom request was $5.3M USD, in which the municipality refused to pay and tried to restore back their data.[5] The third one with the highest ransom request was the attack from January 2020 on Travelex, a British exchange company, got hit by 'Sodinokibi' ransomware which encrypted 5GB of customer data.[6] Hackers demanded £4.6M (which approximates to $6M USD); eventually the company paid $2.3M USD.[7] In all three cases the ransom requests were significant, but still much lower than in the case of Garmin.

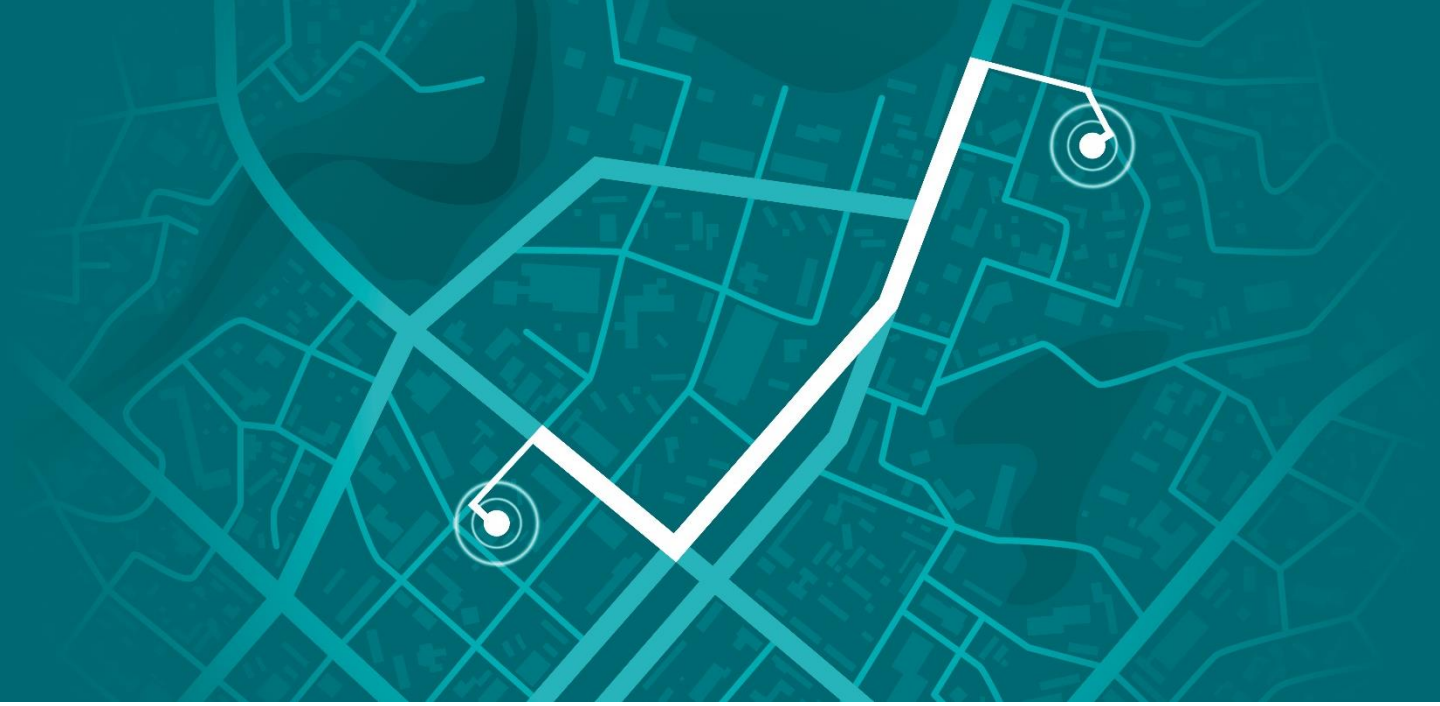
Company	Industry	Ransomware	Ransom Request
Pemex	Mexican oil company	DoppelPaymer	$4.9M USD
New Bedford	Municipality in Massachusetts	Ryuk	$5.3M USD
Travelex	British exchange company	Sodinokibi	$6M USD
Garmin	iOT, Aviation, Technology	WastedLocker	$10M USD

4 https://blog.knowbe4.com/mexican-oil-company-pemex-dodges-5m-ransomware-bullet

5 https://threatpost.com/ransomware-demand-massachusetts-city-no-thanks/148034/; https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/

6 https://www.bbc.com/news/business-51017852

7 https://www.wsj.com/articles/travelex-paid-hackers-multimillion-dollar-ransom-before-hitting-new-obstacles-11586440800



SOME BACKGROUND ABOUT GARMIN

Garmin Ltd. is an American international tech company, founded in 1989. The company produces, designs and sells navigation, communication and information devices and applications, most of which are enabled by GPS technology.[8] Company's main products are smart sport watches, which monitor data for jogging running or other fitness activities such as pulse rate, distance measurement and calorie burning. In addition, Garmin develops navigation systems and smart maps for aviation and the marine sector.[9] Company's net income in 2019 summed up to $952M.[10]

In 2019, Garmin employed 15,000 people in 65 branches around the world.[11] The company has two HQ: the operational HQ is located in Olathe, Kansas, USA and the legal one locates in Schaffhausen, Switzerland.[12] The main production plants are located in Taiwan and China.

8 https://en.wikipedia.org/wiki/Garmin#cite_note-2018IncomeStatement-1

9 https://www8.garmin.com/aboutGarmin/invRelations/reports/2018_Annual_Report.pdf
Garmin Annual Report, 2018, p. 5-21.

10 https://www.dnb.com/business-directory/company-profiles.garmin_ltd.51a095a8ddc52f76775881fb9350c050.html#industry-info

11 https://www.statista.com/statistics/1036207/employee-number-of-garmin/

12 https://en.wikipedia.org/wiki/Garmin#cite_note-2018IncomeStatement-1;
https://www.forbes.com/companies/garmin/#306445fd7d0b

WHO ATTACKED GARMIN?

The Evil Corp group is active since 2007. In the past, they distributed the 'Dridex' Trojan horse, which focused on attacking banking user credentials around Europe and English-speaking countries.[13] In the last few years the group started developing ransomware, such as 'BitPaymer' in 2017.[14]

Since the COVID-19 breakout in March 2020, 'Evil Corp' launched a wide campaign with a ransomware called 'WastedLocker' against 31 American organizations.

The attack was based on Social Engineering exploiting the fact that most corporate employees were working remotely.[15]

Evil Corp has successfully exploited the 'weak spots' that emerged during the 'remote working' period, like weak desktop protocols, weak passwords, lack of cybersecurity training, awareness and others.[16]

The leader of the group, is a 33 year old Russian citizen named Maksim Yakubets. According to the FBI and the DOJ, Yakubets became the most wanted cybercriminal on the FBI cybercrime wanted list. A $5M reward was offered for information leading to his arrest, together with another hacker from the group, named Igor Turashev.[17] Both had links to the FSB, the Russia Federal Security Service.[18]

HOW DOES WASTEDLOCKER WORK?

'WastedLocker' renames files' extension with the word 'wasted'.[19] 'WastedLocker' is also able to adjust to its environment and is looking for different vulnerabilities i.e. has the capability to run multiple exploitation techniques and build different attack scenarios.[20]

> “ MALICIOUS CODE THAT DISABLES THE REAL-TIME MONITORING AND SCANNING OF DOWNLOADED FILES. ”

13 https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=8109b9d1-6435-443a-b033-2df8461f10c7&CommunityKey=f5d62f53-a337-4805-842f-e5bc06329b21&tab=librarydocuments

14 https://www.zdnet.com/article/new-wastedlocker-ransomware-demands-payments-of-millions-of-usd/

15 https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wastedlocker-ransomware-us

16 https://www.zdnet.com/article/ransomware-attacks-jump-as-crooks-target-remote-working/

17 https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens ; https://www.fbi.gov/wanted/cyber/maksim-viktorovich-yakubets ; https://www.fbi.gov/wanted/cyber/igor-olegovich-turashev ; https://www.youtube.com/watch?v=-R0lsczNUN4&t=158s

18 https://krebsonsecurity.com/2019/12/inside-evil-corp-a-100m-cybercrime-menace/

19 https://www.pcrisk.com/removal-guides/18227-wastedlocker-ransomware

20 https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wastedlocker-ransomware-us

ATTACK PHASES

The ransomware is distributed via SocGholish fake update framework, the user downloads a zip file which contains a malicious JavaScript bot which is executed by wscript.exe. The SocGholish JavaScript bot has access to information from the system itself as it runs under the privileges of the browsing user. The bot collects a large set of information and sends it to the SocGholish server side which, in turn, returns a payload to the victim machine.

The payload contains a PowerShell script which is used to download and execute a loader from a domain publicly reported as being used to deliver Cobalt Strike as part of WastedLocker attacks. The loader also shares a command and control (C&C) domain with this reported Cobalt Strike infrastructure.

Also, the loader contains a .NET injector which is reportedly taken from an open-source project called Donut, which is designed to help inject and execute in-memory payloads, the injected payload is known as Cobalt Strike Beacon and can be used to execute commands, inject other processes, elevate current processes or impersonate other processes, and upload and download files.

In order to deploy the ransomware, attackers use PsExec to control windows defender via a command line tool (mpcmdrun.exe) so they can disable the scanning of downloaded files and in some cases, disable real-time monitoring, and also to launch PowerShell which uses the win32_service WMI class to stop services across the organization.

After Windows Defender is disabled and services have been stopped across the organization, PsExec is used to launch the WastedLocker ransomware itself, which then begins encrypting data and deleting shadow volumes.

IS RANSOMWARE PAYMENT TAX DEDUCTIBLE?

As mentioned above, the costs of ransom are very high and can reach millions of dollars. Related to this, the question arises whether a company that has decided to submit to the demands of the attackers and pay the ransom, may request a tax deduction for the expenditure. Income Tax laws allow the taxpayer to deduct an expense if it has been proven that the expense involved was incurred while trying to generate income and that the expense was actually paid.

In this regard, it is important to remember that payments which are associated with a violation of any law, are not deductible as an expense. The intention is mainly to apply to bribe payments, etc. Should the payment of the ransom be the same as the payment of a bribe? In our humble opinion the unequivocal answer is no. The payment of the ransom is similar to any other business expense and there is no connection between it and a non-deductible fines or illegal payments.

The problems that need to be overcome in this matter, are related to the proof of payment (the attacker will probably not issue a receipt for the payment) and to issues of tax withholding. At the same time and in light of the fact that this is a payment, which as stated is related to the day-to-day operation of the business and reduces the business profits unilaterally, we believe that (subject to obtaining a professional opinion), this expense can be deducted from the company's taxable income. It is clear that this opinion applies globally, but it is important to add that the specific local tax laws in each country must be examined to ensure that there is no law that prohibits this. Logically speaking, the answer is “yes”.

FALLOUT - CLASS ACTION LAWSUIT

It was reported on Monday, August 10th, that due to the ransomware attack, Garmin's clients in Israel filed a class action lawsuit in Tel Aviv District Court against Garmin Company and against Ronlight Digital Ltd, Garmin's exclusive importer in Israel. The total claim summed up to 52M NIS (more than $15.2M USD). The background of the lawsuit is that the defendants violated customer's property and privacy rights.[21]

21 https://www.ynet.co.il/digital/technews/article/Ske11tdpbv

CONTACTS:

OPHIR ZILBIGER
Partner
Head of Cybersecurity Center
BDO Israel
OphirZ@bdo.co.il

NOAM HENDRUKER
Partner
Head of Global Cyber Consulting Group
BDO Cybersecurity Center, Israel
NoamH@bdo.co.il

GUY RESHTICK
Partner
Corporate Tax, CPA
GuyR@bdo.co.il

TOMMY BABEL
Senior Manager
Head of Cyber Reselience Services
BDO Cybersecurity Center, Israel
TommyB@bdo.co.il

This publication has been carefully prepared, but it has been written in general terms and should be seen as broad guidance only. The publication cannot be relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact BDO Israel to discuss these matters in the context of your particular circumstances.

BDO Israel, its partners, employees and agents do not accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

BDO Israel, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independence Member Firms.

BDO is the brand name for the BDO network and for each of BDO Member Firms.

For further information about how BDO can assist you and your organization, please visit **www.bdo.co.il**