deepinstinct™
BEFORE YOU KNOW IT

PREVENTION IN ACTION

CASE STUDIES | 2020

CYBER ATTACK PREVENTED

GandCrab Ransomware

1

OVERVIEW

- GandCrab is one of the most prevalent ransomware threats of the last two years. GandCrab has had at least nine unique versions, as of June 2019, and each version can mutate into thousands of unique variants.
- In June 2019 the operators of GandCrab said they are ending the operations of the ransomware, after stating they earned around $2.5M per week from their operations.
- GandCrab ransomware variants have affected more than 1.5 million users of the Windows Operating System, and the cyber criminal organization claimed they collected more than $2 billion in ransomware extortion payments.
- At least some of the actors behind GandCrab are suspected of being involved in the development and distribution of a new family of ransomware called Sodinokibi. This ransomware rose to prominence in mid-2019 and has since caused heavy damage to organizations. MSP Applications were exploited by the actors to attack a large number of organizations, and the ransomware is also suspected to be involved in many more high-profile attacks.
- GandCrab ransomware is considered to be one of the most largely distributed ransomware variants globally, affecting both small businesses and large enterprises alike.

2

WHERE IT WAS DETECTED AND PREVENTED

GandCrab Ransomware was detected and prevented from causing any damage by Deep Instinct, in a large and well-known aviation company that operates international flights out of Asia.

GandCrab was initially detected as a copy in a system not protected by Deep Instinct's solution. It was caught as it attempted to spread via the SMB port in to any enivronment that was protected by Deep Instinct.

3

IMPACT OF THE THREAT IF EXECUTED

If the ransomware were to be executed successfully at the customer site, it could have caused a major disruption to flight operations. For example, flight schedules would have been disrupted as ground crew would not have been able to manage customer boarding details. Case systems related to customer bookings could have been attacked, whereby customer booking data would have been lost, and new bookings could not be made for future flights.

If not prevented pre-execution, the air flight company would have struggled to disable the attack, to be effective it would need to have detected the remote desktop protocol attack, where the perpetrators first scan a given network for systems that are set up for remote access. Once the attackers have scanned the network they identify the target files to zero-in on. Once GandCrab is executed, files are encrypted in moments, leaving no time for an EDR solution to react.

The impact of disabling these activities would cause major financial loss that would run into millions of dollars, not to mention the difficult-to-restore reputational damage to the airline company.

4

PREDICTION OF COSTS, SHOULD THE RANSOMWARE HAVE BEEN ALLOWED TO INFILTRATE

Business Downtime On the expectation that 10% - 20% of files would be brought down for 10 days, this would cause $8 to $16 million in lost revenue

Ransom Demand Considering the size of the company and the expected survival math, the ransom demand could be anywhere between $30,000 - $50,000

Regulatory Risk The relevant civil aviation authority, for the flight company's jurisdiction, could impose fines for denied boarding, delay and the cancellation of flights. Fines range between 250€ to 600€ per passenger, depending on the distance of the flight

Reputational Damage Increases in proportion to the frequency of being attacked which according to FBI statistics there are 4,000 attempted attacks per day. This takes its toll on reduced business as customers perceive the company to be unsafe to deal with

Theft of Computing Resources The encryption of files consumes processing power to the effect of creating a discernable lag time

Operational Costs Considering the number of endpoints, across global locations, the cost would have been in the millions of dollars

$16M

TOTAL POTENTIAL LOST REVENUE

5

SO, WHAT HAPPENED IN THE END?

With Deep Instinct's solution installed, no action was required from the customer.

Deep Instinct's deep learning-based security product prevented the malicious dropper from executing and downloading additional payloads. Since the solution prevented the attack pre-execution, the dropper and the ransomware payload never made its way into the customer environment.

6

FURTHER REMEDIATION ACTIVITIES

GandCrab was automatically analyzed to provide forensic data on classifying the ransomware and further details on how it operates. The analysis showed the infection vectors of GandCrab include drive-by downloads from compromised web-sites, phishing e-mails containing socially engineered documents, while some infections are caused by browser attacks carried out with exploit kits.

PREVENTION IN ACTION

BANKING

deepinstinct™
BEFORE YOU KNOW IT

CYBER ATTACK PREVENTED

Nanocore Remote Access Trojan (RAT)

1

OVERVIEW

- The NanoCore RAT was developed in 2012 and appeared quite extensively in the wild in 2013, where it was being sold online for around $20.
- NanoCore offers numerous spyware functionalities, such as keylogging, sound and webcam capture, and backdoor access. The RAT also includes various network functions, which enable attackers to collect network information, and communicate covertly with the infected computer.
- NanoCore was tied to attacks in many countries, including targeted attacks against energy firms in the Middle East and Asia. The RAT was also used in numerous other attacks, including many waves of phishing emails in attempts to compromise business organizations.
- The developer behind NanoCore was arrested in late 2016, and in February 2018 was sentenced to 33 months in prison.

2

WHERE IT WAS DETECTED AND PREVENTED

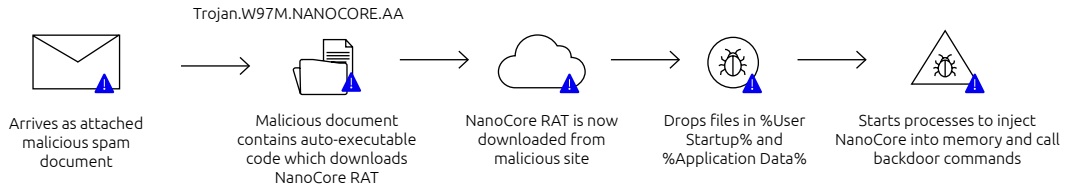
NanoCore RAT was detected and prevented by Deep Instinct in a large West European online bank. The bank is a leader in online stock market information, and services both private and professional investors.

The NanoCore RAT was detected arriving at the customer environment in the form of an attached malicious spam Word document which the Deep Instinct D-Client prevented from downloading.

3

IMPACT OF THE THREAT IF EXECUTED

If allowed to execute, the malicious document dropper contains auto-executable code which downloads the NanoCore RAT. Once downloaded from the malicious site it drops files in %UserStartup% and %AppData%. This then triggers processes to inject NanoCore RAT into memory and perform additional commands.



If not prevented pre-execution it would have been difficult, if not impossible, to stop the backdoor from getting a foothold within the bank's network. Within minutes the backdoor can execute a credential theft pick-up and send all saved passwords to its C&C server. Considering the malware's sophisticated evasion capabilities, NanoCore can persist within a remote location for days, if not months, as SOC teams struggle to kill its processes. The more time it gains within the remote systems the further its tentacles can spread to wreak more damage.

In the past few years, several sophisticated attack groups have targeted banks, using various types of malware for initial access, including RATs. In these similar attacks, the hackers were able to gain initial access, and then install additional malware which compromised SWIFT transfers or ATM machines. One example among many occurred in February 2019, where the Bank of Valletta in Malta closed its operations after an attempted theft of €13 million by cyber attackers.

4

PREDICTION OF COSTS, SHOULD THE RANSOMWARE HAVE BEEN ALLOWED TO INFILTRATE

Business Downtime NanoCore RAT can persist in a remote location from varying durations of time, anywhere between days to months. While the information-stealing trojan is not likely to cause a direct business closure, the remediation process could. Business downtime due to remediation would be most severe in the time just after attack, and gradually minimize with time. For a company this size the lost business could accumulate to millions of dollars.

Regulatory Risk The data theft capability compromises customer data security, considering the bank is based in the EU, it would be subject to the regulatory requirements of GDPR (General Data Protection Regulation) for which the penalty for non-compliance is up to €10 million or 2% annual global turnover, depending on the severity of the breach.

Reputational Damage A survey conducted by OnePoll found that from amongst their 2000 respondents 86.55 percent were "not at all likely" or "not very likely" to do business with an organization that had suffered a data breach involving financial details. This number lowered slightly if other data points, such as email addresses, had been stolen.

Theft of Computing Resources The ability to disable usage capabilities could potentially undermine the operability of infected computing resources, putting all endpoints across the enterprise at risk.

Operational Costs If the 1,200 endpoints being protected by Deep Instinct had been breached, the response and remediation costs could range anywhere between $200,000 to $2.5 million.

UP TO

$2.5M

IN RESPONSE AND REMEDIATION COSTS

5

SO, WHAT HAPPENED IN THE END?

With Deep Instinct's solution installed, no action was required from the customer.

Deep Instinct's deep learning-based security product prevented the RAT from executing and downloading additional payloads. Since the solution prevented the attack pre-execution, the RAT never made its way into the customer environment.

6

FURTHER REMEDIATION ACTIVITIES

NanoCare RAT was automatically analyzed to provide forensic data on classifying the malware and further details on how it operates.

PREVENTION IN ACTION

EDUCATION

deepinstinct™
BEFORE YOU KNOW IT

1

OVERVIEW

CYBER ATTACK PREVENTED

PONY STEALER

- Pony Stealer is a spyware that has been in the wild since 2011.
- According to The Credential Theft Ecosystem Report it is the most threatening credential stealing trojan that targets popular applications and browser data.
- In December 2012 Pony's source code was leaked, and due to this decentralization, it became widespread on the darknet. This proliferation greatly contributed to making Pony a more difficult threat to mitigate compared to its rival stealers.
- Pony is mainly distributed via phishing email campaigns as well as exploit kits and can be also used as a dropper of other malware variants.
- This malware has been responsible for several high-profile attacks, one of them being the theft of almost two million sets of credentials from Facebook, Twitter, Yahoo Google and the ADP payroll service.
- Its 2014 campaign resulted in the theft of 700,000 sets of credentials and $200,000 in stolen cryptocurrencies.
- In 2015 Pony Stealer was used to deliver the ransomware program 'CryptoWall' which successfully encrypted hundreds of web pages globally.
- Prone to targeting educational institutions, in July 2019 the US Department of Education issued a statement that 62 colleges and universities were hit by Pony Stealer which had exploited a vulnerability in a popular education-related software. The exploit was used to create hundreds of fake student accounts, yet the purpose of these fake accounts was not disclosed.
- In the same month, the records and ID documents of students at Lancaster University were compromised by attackers.

2

WHERE IT WAS DETECTED AND PREVENTED

Pony Stealer was detected in a large and well-known tertiary institution that has several campuses throughout Canada. With 4,000 endpoints sold, so far 1,500 have been deployed.

Pony Stealer was initially detected as a malicious link in a drive-by-download from where it would have exploited the browser or operating system to infiltrate the system.

3

IMPACT OF THE THREAT IF EXECUTED

If the spyware had executed inside the tertiary institution, the Pony Stealer could have begun to collect sensitive data such as user credentials, including the credentials of privileged administrative users. Once such credentials are obtained, they could be used by the malware to gain control of the organization's network and perform a variety of actions to achieve their malicious objectives, such as stealing the organization's sensitive data and IPs, or downloading and deploying ransomware.

If not prevented pre-execution, the Pony would have infiltrated the system through the drive-by download. Pony Stealer operates behind systems collecting information; about its infrastructure, its network activity, data points about connected users and their user credentials. It then transmits this information to its command and control server. After the theft, it can be designed to self-terminate or continue dormant as a stand-alone executable.

Pony Stealer can be used to load additional malware onto the target system. In more sophisticated attacks, it is combined with several different types of malware. Particularly devastating techniques have involved attackers using phishing techniques to trick users into downloading a Pony, and then once in the system, the Pony is used to download malware to mount further attacks.

Pony can also be used as a Botnet controller. Once it has infected the computer, the botnet can recruit it to launch attacks on other victims.

4

PREDICTION OF COSTS, SHOULD THE RANSOMWARE HAVE BEEN ALLOWED TO INFILTRATE

Business Downtime A Pony Stealer can persist in a remote location from varying durations of time, anywhere between days to months. While the information-stealing malware is not likely to cause a direct business closure, the remediation process would. For an educational institution of this size, any business downtime would cause enormous frustration among faculty staff causing losses that would reach hundreds of thousands of dollars.

Regulatory Risk The data theft capability compromises student data security, considering the federally-regulated college is based in Canada, it is subject to The Personal Information Protection and Electronic Documents Act (PIPEDA). If the College does not comply with the standards, it can be issued a fine of up to $100,000

Reputational Damage If breached, the students would be the most badly impacted, the reputational damage could impact enrollments by as much as 10% for the following year.

Operational Costs Considering Pony Stealer's ability to spread undetected, there would have been a huge number of endpoints infected across the college's multiple campuses. The cost to respond and clear the enterprise of residual malware would be in the millions of dollars.

$1M+
IN POTENTIAL REMEDIATION COSTS

5

SO, WHAT HAPPENED IN THE END?

With Deep Instinct's solution installed, no action was required from the customer.

Deep Instinct's deep learning-based security product prevented the malicious dropper from executing and stealing data. Since the solution prevented the attack pre-execution, the dropper never made its way into the customer environment.

6

FURTHER REMEDIATION ACTIVITIES

Pony Stealer was automatically analyzed to provide forensic data on classifying the malware and further details on how it operates.

1

OVERVIEW

CYBER ATTACK PREVENTED

EMOTET MALWARE

As one of the world's most constantly evolving malware, Emotet has become a perpetual source of challenge to organizations globally. It first appeared in German speaking countries in Europe around mid-2014, and reappeared targeting the UK and US with amplified capabilities in 2017 after 2 years without significant activity.

From its very first version, Emotet spread mainly via spam campaigns, imitating financial statements, transfers and payment invoices. Once it is dropped and run, Emotet intercepts and logs network traffic, injects code into browsers and tries to access banking sites in order to steal and store financial data.

No delicate wall-flower, Emotet has been the cause of some serious damage. In July 2019 Emotet was used in a ransomware attack against Lake City, Florida which demanded a payout of $460,000. It then lashed out in September of 2019, targeting German, Polish, Italian and English companies through emails with deceptive subject lines like "Payment Remittance Advice" and "Overdue Invoice". Once the infected Microsoft Word document initiates a Macro, it downloads Emotet.

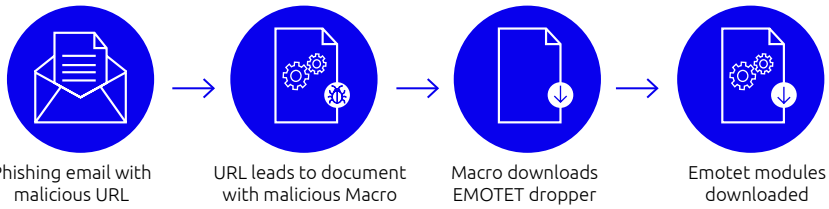
The banking trojan gradually transitioned from malware, which is more financially focused, to a botnet which is used to download additional malware, such as Trickbot or ransomware. As a botnet, it accounts for almost two thirds of all malware payloads delivered by email, with a preference for malicious URL's rather than weaponized attachments. The malware authors continuously improve the droppers, payload and distribution mechanisms, all contributing to its widespread proliferation which other malicious campaigns have used to hitch a ride on.

2

WHERE IT WAS DETECTED AND PREVENTED

Emotet Malware was detected and prevented by Deep Instinct in a large Managed Security Services Provider (MSSP) that provides IT support to small and medium sized businesses in the USA.

Emotet was initially detected as a scam phishing email. Following its typical behavior, it was accompanied by an attached Word document that was used to execute Macros, which then executes a Powershell. The Powershell is intended to download the next stages of the attack.



Recently, there have been several high-profile ransomware attacks against MSSPs. Though the attacks were ransomware, and not financial malware, they demonstrated how much damage an attacker can do once initial access to an MSSP is gained. Read more about these attacks, and on how to protect yourself when working with an MSSP.

3

IMPACT OF THE THREAT IF EXECUTED

If successfully executed within an MSSP, the effects of financial malware could be particularly severe as the botnet can be purposed towards dropping any type of malware. The malware could steal the banking and credit card details of the organization, leading to reputational and financial damage. In addition, since the malware opens a backdoor for attackers, attackers might also be able to harvest passwords from within the organization and gain access to all the MSSP tenants. In effect, by attacking key spots within an MSSP, attackers could then reach a much wider attack base, by staging attacks against the tenants of the MSSP, from an initial foothold within the original MSSP.

4

PREDICTION OF COSTS, SHOULD THE RANSOMWARE HAVE BEEN ALLOWED TO INFILTRATE

Business Downtime The impact of disabling the activities of this large MSSP would have cause major financial loss that would run into millions of dollars. This could have potentially also cause business downtime for effected tenants, extending the magnitude of loss.

Regulatory Risk The data theft capability compromises tenant data security. On a global level the MSSP would be subject to GDPR and on a Federal level they would be subject to the California Consumer Privacy Act and Federal Laws relating to mishandling of data. If the MSSP was found to not having responded responsibly to the breach, they could be subject to millions of dollars' worth of fines.

Reputational Damage An Emotet breach would cause difficult-to-restore reputational damage to the MSSP, particularly, if tenant environments were impacted. The damage could result in the termination of contracts with existing clients and impact loss of business, by as much as 10% in the following 12-month period.

Operational Costs Depending on the number of endpoints affected, not just within the MSSP, but also those of tenant environments located globally, the operational cost of responding and remediating would be in the millions of dollars.

5

SO, WHAT HAPPENED IN THE END?

With Deep Instinct's solution installed, no action was required from the customer.

Deep Instinct's deep learning-based security product prevented the malicious document dropper contained in the spam email and the executable payload which is downloaded by the dropper. Since the solution prevented the attack pre-execution, the document dropper and the executable payload never made its way into the MSSP or the environment of any of its tenants.

6

FURTHER REMEDIATION ACTIVITIES

Emotet was automatically analyzed to provide forensic data on classifying the malware and further details on how it operates.

$1M+

IN OPERATIONAL COSTS

PREVENTION IN ACTION

RETAIL

deepinstinct™
BEFORE YOU KNOW IT

1

OVERVIEW

MALWARE IDENTIFIED

CRYPTOWALL RANSOMWARE

- CryptoWall is a ransomware family active since 2014 and is considered one of the first highly prolific strains of ransomware. In the first years of its campaign it infected over 600,000 endpoints and stole over $1,101,900 US in paid ransom.
- Nearly two thirds of ransom demands paid $500, but the amounts ranged from $200 to $10,000.
- CryptoWall gained its reputation by placing malicious advertisement on commonly used domains such as Facebook, Disney, The Guardian, and others, which upon being clicked on, led people to sites which were infected by CryptoWall and encrypted their drives.
- CryptoWall can be executed on both 32-bit and 64-bit systems. This flexibility increases its chance of the malware running on whichever computer it happens to infect.

2

WHERE IT WAS DETECTED AND PREVENTED

CryptoWall was detected and prevented by Deep Instinct in a medium sized supermarket chain in the United States. The supermarket has a number of chains each with their own servers and registers that all stored customer credit card numbers among other sensitive information and required protection.

The CryptoWall ransomware was detected arriving at the customer environment in the form of an attached malicious spam ZIP attachment where the virus was hidden in PDF files which the Deep Instinct D-Client prevented from downloading.

3

IMPACT OF THE THREAT IF EXECUTED

Once allowed to execute, the ransomware encrypts dozens of different file types on infected computers. When a victim opens the malicious PDF files, the computer becomes infected with the CryptoWall ransomware which installs malware files either in the %AppData% or %Temp% folders. Once the computer is infected the malware will begin snooping around the computer's drives for data files in can encrypt. Finally, while the malware is scanning the computer, it will locate drive letters on the PC including shared networks, Dropbox mappings and removable drivers – any drive letters present on the computer will be scanned for data files.

In previous attacks on the retail sector CryptoWall has left a trail of destruction:

- The average financial loss as a result of a single cyberattack costs a retailer $1.6 million.
- 77% of retail executives admitted their current security strategies were influenced by having already suffered a data breach of this scale.
- About 66% of companies in the retail sector admitted to paying the ransom to a hacker within the last year.

4

PREDICTION OF COSTS, SHOULD THE RANSOMWARE HAVE BEEN ALLOWED TO INFILTRATE

- **Business Downtime** If the ransomware were to be executed successfully within the supermarket's network, it could have created a major disruption in purchase operations. For example, cash registers could have been disrupted as the files in them would have been encrypted. If case systems required for inventory supply were attacked, supplies would not have reached the retail store and online orders would not have been delivered to customers.
- **Ransom Demand** Considering the size of the company, the typical demands for this ransomware and the expected survival math, the ransom demand would be anywhere between $500 - $5,000.
- **Regulatory Risk** The data theft capability compromises customer data security, considering the Supermarket is based in the USA, it would be subject to the regulatory requirements of GDPR (General Data Protection Regulation). On a Federal level they would be subject to the California Consumer Privacy Act and Federal Laws relating to mishandling of data. If the Supermarket chain was found to not having responded responsibly to the breach, they could be subject to millions of dollars worth of fines.
- **Reputational Damage** A survey conducted by OnePoll found that from amongst their 2000 respondents' 86.55 percent were "not at all likely" or "not very likely" to do business with an organization that had suffered a data breach involving financial details. As the breach was focused on stealing credit-card numbers, this would have been a huge hit on the public's perception as the supermarket being a safe place to shop.
- **Theft of Computing Resources** The encryption of files consumes processing power to the effect of creating a discernable lag time.
- **Operational Costs (responding and remediating attacks, impact on operations)** In this customer environment Deep Instinct has 679 agents deployed, and if only one of the machines had been breached, the response and remediation costs could have ranged anywhere between $200,000 to $1.5 million.

$200,000 TO $1.5
In remediation costs

5

SO, WHAT HAPPENED IN THE END?

With Deep Instinct's solution installed, no action was required from the customer.

Deep Instinct's deep learning-based security product prevented the dropper from executing and downloading the malware payloads. Since the solution prevented the attack pre-execution, the malware never made its way into the customer environment.

6

FURTHER REMEDIATION ACTIVITIES

CryptoWall was automatically analyzed to provide forensic data on classifying the malware and further details on how it operates.

1

OVERVIEW

MALWARE IDENTIFIED

RYUK RANSOMWARE

- Ryuk is a ransomware family that threatens in some cases to publish the victim's data, while perpetually blocking access to it until a ransom is paid.
- Attacks tend to be highly targeted against English speaking users from companies which they select one at a time, either via spear phishing emails or Internet-exposed and poorly secured RDP connections.
- First identified in October 2018, several updates of Ryuk have appeared since its release, and in one of its latest updates, in September 2019, Ryuk was programmed to steal confidential military, financial, and law enforcement files.
- Ryuk ransomware was first seen in the wild in August 2018 and has since been involved in numerous high-profile ransomware incidents, such as attacks against Florida municipalities, which netted the criminals more than $1.1M.
- Once infecting a system, Ryuk has established a pattern of killing over 40 processes and stopping more than 180 services, before beginning to encrypt files. Additionally, Ryuk requires admin privileges to run, therefore it maintains persistence by writing itself to the Run registry key.
- Ryuk is often distributed as a secondary payload of Emotet or Trickbot, which are spread through spam emails.

2

WHERE IT WAS DETECTED AND PREVENTED

Ryuk was detected and prevented by Deep Instinct in a private hospital located in Southeast Asia. The over 200 bed facility has 3,500 agents deployed across multiple types of endpoints that are used cross-functionally amongst the 4,800 people employed at the international hospital. The hospital invested heavily in the digitization of patient information by utilizing an integrated hospital information system that uses electronic medical records and digital radiology systems. The Deep Instinct appliance is configured to protect Windows OS, MacOS and Android devices with 2.2 based versions

Ryuk was detected arriving as a secondary payload accompanied with an already existent Emotet installation. The payload was delivered through a malicious spam DOCX attachment where the virus was hidden in the document which the Deep Instinct D-Client prevented from downloading.

3

IMPACT OF THE THREAT IF EXECUTED:

If successfully executed within the hospital, the effects of Ryuk ransomware could be particularly devastating as its encryption methods are highly effective with the potential for shuttering entire network systems, potentially putting human lives at risk. On October 1st, 2019 Druid City Hospital (DCH) Health System and their Regional Medical Centers were infected by Ryuk. The ransomware caused the closure of their entire computer systems, forcing the health system to stop accepting new non-emergency patients.

DCH issued a statement updating the public on the incident, which advised that while some systems were being restored from back-ups, they were also paying the ransom and had purchased the Ryuk decryption key in order to restore more access to other systems still encrypted. While the hospital did not disclose how much the ransomware fee was, they did advise that the decryptor key was successful in decrypting the server.

According to CSO online the developers of Ryuk target hospitals to "exploit the fact the organizations provide life-saving services and therefore could be more inclined to pay". In another ransomware attack the California-based Wood Ranch Medical blamed a ransomware attack that occurred on August 10, 2019 on its decision to close permanently in December of that year.

$1M
In remediation costs

4

PREDICTION OF COSTS, SHOULD THE MALWARE HAVE BEEN ALLOWED TO INFILTRATE

- **Business Downtime** The impact of disabling the activities of this private hospital would primarily put patient safety at risk, as doctors would not be able to reference digital medical charts and notes. Major financial loss would also be incurred, running into millions of dollars, depending on how long it would take to restore systems.
- **Ransom Demand** ($ Loss) Considering the size of the hospital and the expected survival math, the ransom demand would be anywhere between $30,000 - $50,000[1]
- **Regulatory Risk** The relevant Ministry of Public Health, that has jurisdiction in the hospital's region, could impose fines for compromised patient care and breach of patient trust, if it was found that the hospital did not respond to the ransomware threat in an efficient and ethical manner. Fines range between $250 to $600 (in equivalent USD) per patient, depending on the severity and impact of neglect .[2]
- **Reputational Damage** A Ryuk ransomware outbreak would cause difficult-to-restore reputational damage to the hospital, particularly, if the impact on patient care was severe. The damage could result in the reduced number of new patients, and the loss of health accreditations, which in the worst-case scenario, could force closure.
- **Operational Costs** Depending on the number of endpoints affected, the operational cost of responding and remediating would be in the millions of dollars .[3]

1 https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread
2 http://www.fda.moph.go.th/sites/fda_en/SitePages/Medical.aspx?IDitem=LawsAndRegulations
3 https://www.malwarebytes.com/emotet/

5

SO, WHAT HAPPENED IN THE END?

With Deep Instinct's solution installed, no action was required from the customer.

Deep Instinct's deep learning-based security platform prevented the malicious document dropper contained in the spam email and the executable payload which is downloaded by the dropper. Since the solution prevented the attack pre-execution, the document dropper and the executable payload never made its way into the hospital.

6

FURTHER REMEDIATION ACTIVITIES

Ryuk was automatically analyzed to provide forensic data on classifying the malware and further details on how it operates.

ABOUT DEEP INSTINCT

Deep Instinct is changing the way we look at cybersecurity by harnessing the power of Deep Learning to prevent threats in zero time. Deep learning is inspired by the brain's ability to learn. Once a brain learns to identify an object, its identification becomes second nature. Similarly, as Deep Instinct's artificial deep neural network brain learns to prevent any type of cyber threat, its prediction capabilities become instinctive. As a result, any kind of malware, known and new, first-seen malware, zero-days, ransomware and APT attacks from any kind are redirected and prevented in zero time with unmatched accuracy and speed anywhere in the enterprise —Network, EPP, Mobile—enabling a multilayered protection.

Request an online demonstration of Deep Instinct's solution.

Click here to set up a free consultation on your endpoint security environment and see how Deep Instinct can help protect your organization in this live demonstration of our solution capabilities.

Request a Demo

GET STARTED WITH THE CYBERSECURITY REVOLUTION

ISRAEL
23 Menachem Begin Rd
28th Floor
Tel Aviv
Israel, 6618356

UNITED STATES
501 Madison Ave
Suite 1202
New York City, NY
USA, 10022

UNITED KINGDOM
5 Ribbon Pond Drive
Newark on Trent
Nottinghamshire
NG24 3WW

+972 (3) 545-6600 www.deepinstinct.com contact@deepinstinct.com