# Ransomware: What Lies Ahead?

## A Comprehensive Guide for Sophisticated Ransomware Variants

6 September 2016

# Where Are the Most Sophisticated Ransomware Variants Heading?


| | | |
|---|---|---|
| #1 | Executive Summary | 3 |
| #2 | Introduction | 5 |
| #3 | Classic Crypto Ransomware Behavior | 11 |
| #4 | Unique Ransomware Behavior | 14 |
| #5 | Trends and Forecast | 18 |
| #6 | Conclusion: Steps to Avoid Becoming a Ransomware Victim | 28 |
| #7 | References | 33 |

# #1 Executive Summary

The rise of ransomware appeared in every major industry forecast for 2016. Unfortunately, this prediction has materialized. Ransomware keeps appearing in headlines; attacking hospitals, banks, school districts, state and local governments, law enforcement agencies, as well as businesses of all sizes. Ransomware is reaching an epidemic level. The number of people targeted by ransomware is staggering: In the U.S. 4.1% of the population or 13.1 million; Germany: 3.8%, or 3.1 million; France: 3.3%, or 2.2 million; and in the U.K. 2.6%, or 1.7 million. Cyber-criminals collected $209 million in the first three months of 2016 from ransomware.

This paper is the result of Deep Instinct's detailed research into classic and unique ransomware families. Its purpose is to provide a solid foundation for developing protective measures in your organization. Reading this paper offers a thorough understanding of the different types of ransomware, how it can be created and the course of its evolution, especially as it expands into new territories such as mobile devices and IoT.

## Upon Reading this White Paper, Cybersecurity Teams Will Learn:

- What are the different types of ransomware?
- What are the trends and forecasts for ransomware?
- How to prevent falling victim to ransomware attack?
- How to minimize the damage from a ransomware attack?
- What to do if your organization fell victim to a ransomware attack?

# #2 Introduction


What is Ransomware? 6

The State of Ransomware Attacks 6

Ransomware Types 8

The Evolution of Ransomware (Infographics) 9

Attack Vectors 10

# What is Ransomware?

Ransomware is a type of malware used to extort money. It denies access to the organization's or individual's data (most commonly by encrypting it), holding it for ransom. The payment is usually demanded in Bitcoin, in return for a decryption key that "frees" the seized data. Ransomware has evolved to incorporate a wide range of tactics and methods of holding data ransom. Its attacks have spread from PCs to mobile devices and IoT.

## The State of Ransomware Attacks

Ransomware has come to be viewed as an epidemic, expanding to more attacks on mobile devices and even IoT.

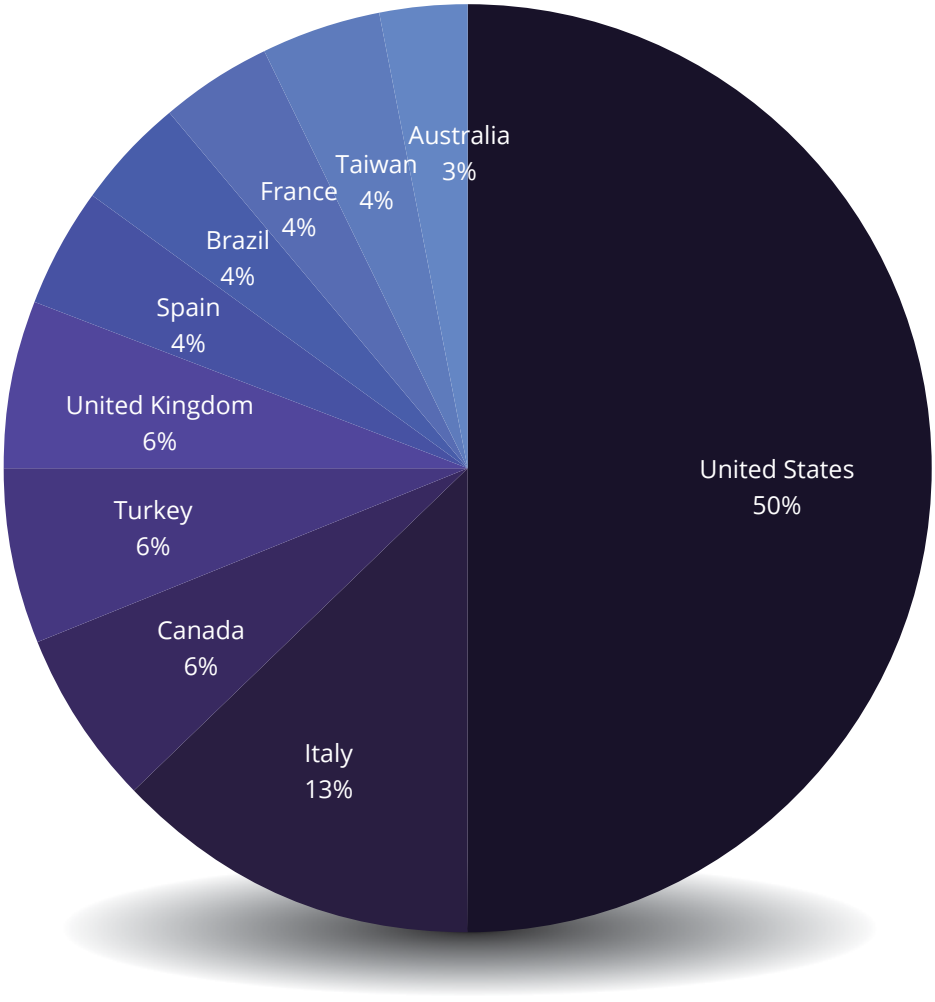
Having appeared in almost every industry trend forecast for 2016, ransomware proved to be one of the biggest threats, wreaking havoc on big and small businesses alike, across industries. The total number of users who encountered ransomware from April 2015 to March 2016 grew by 17.7% in comparison to the previous year.

The rise of ransomware is the outcome of the continued growing sophistication of Crime as a Service (CaaS) with criminal organizations adopting corporate structures, having a developed market of services on the Darknet, and being able to outpace enforcement agencies. There are many reasons for the proliferation of ransomware: it is an opportunistic threat that does not necessarily require any coding skills because kits can be bought on the Darknet. Additionally, since the risk of getting caught is low and with the high profits gained, the ROI is extremely high.

## Large-scale ransomware attacks during March – May 2016


*Large-scale ransomware attacks during March – May 2016*
*Source: https://blogs.technet.microsoft.com/mmpc/2016/05/18/the-5ws-and-1h-of-ransomware/*

## Top 10 countries with the most ransomware detections during December 2015 – May 2016




*The top 10 countries with the most detections December 2015 – May 2016*
*Source: https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx#what*

# The Three Ransomware Types

Ransomware is typically delivered through phishing emails, drive by downloads or malvertising.
There are a few types of ransomware:


## Crypto Ransomware

Variants that encrypt data on an infected host, and demand ransom in exchange for decrypting it. This is currently the most common ransomware type in the wild. The success of this ransomware, such as CryptoWall that belongs to this category, has provided a blueprint for aspiring ransomware developers, contributing largely to the increasing profit margins from ransomware, as well as the sustainability of these ransomware "campaigns". Furthermore, the accessibility of strong and reliable encryption algorithms aided the rise of the crypto genre.

## Locker/Lock-Screen Ransomware

Variants that deny access to the infected host and extort the victim for money in exchange for "releasing" it. Such variants are particularly popular among mobile ransomware.

## Rogue Security Software: Fake AVs

Programs that "warn" the user against malware, which has already allegedly infected the host and can only be removed by purchasing the malicious "security software". While many of these fake AVs are harmless (just a bit annoying) and could be considered as PUA (Potentially Unwanted Applications), some variants are becoming more aggressive, leaving no choice other than purchasing the AV, often practically behaving as locker ransomware.

Crypto ransomware is by far the most popular type of ransomware, increasing by 50% in Q1 of 2016. This year alone, there has been a 550% increase in encryption ransomware attacks in the U.S., compared to the same period in 2014-2015. In the U.K., it accounted for 100% of enterprise infections in February and 99% in January.

# The Evolution of Ransomware


Ransomware has evolved from simple malware that blocks or encrypts data to more specialized attacks that incorporate new features, posing bigger challenges on prevention and damage mitigation.

# Ransomware Attack Vectors

**Exploits (mostly via exploit kits):**

Exploit kits are usually hosted in malicious or compromised websites. They are designed to exploit vulnerabilities in client hosts that interact with them, in order to execute malicious code and infect clients with malware. Some well-known exploit kits that spread ransomware are Angler and Neutrino. According to Talos Intelligence, Angler exploit kit targeted 90,000 victims per day, and 62% of its infections deliver ransomware.

**Network Shares**

A method of spreading malware throughout networks by copying the file which executes the malware to network shares (mostly disguised). As a result, other users with access to the network share could get infected.

**Droppers**

A type of malicious code that is designed to install other malware on a target system. The malware code can be contained within the dropper, or downloaded from an external resource once the dropper is activated. Nemucod, for instance, is a ransomware dropper that usually attempts to download the well-known variants TeslaCrypt or Locky.

**Malicious Advertisements (Malvertising)**

Malicious code that is planted in online advertisements. This way, even visiting trusted websites can expose visitors to threats, via third-party ad content displayed on these websites. Website visitors do not necessarily have to click on ads in order to get infected, and might get auto-redirected to malicious websites. This can be seen in the example of the popular website Teepr, which was a victim of malvertising. In April 2016, it redirected visitors to the Angler exploit kit. After a successful infection, the victim was served CryptXXX ransomware (it should be noted that Teepr has over 2 million daily page views and 800K unique visitors per day).

**Spam & Phishing / Spear Phishing:**

Targeted (spear phishing) or non-targeted (phishing) are attempts to mislead users into clicking on malicious links or downloading a malicious attachment. This attack vector uses social engineering to lead the victims to believe that the link/attachment/email is legitimate, and lure them into clicking on the link or downloading the attachment, executing the malicious code causing the attack. This can be achieved by pretending to be a colleague/friend/service provider/ even a governmental authority.

The damages caused by ransomware range from disruption of operations, data loss or data corruption to financial losses. According to Clearswift, 2,500 cases of ransomware attack in the U.S. alone, costing victims $24 million, were reported to the Internet Crime Complaint Center during 2015.

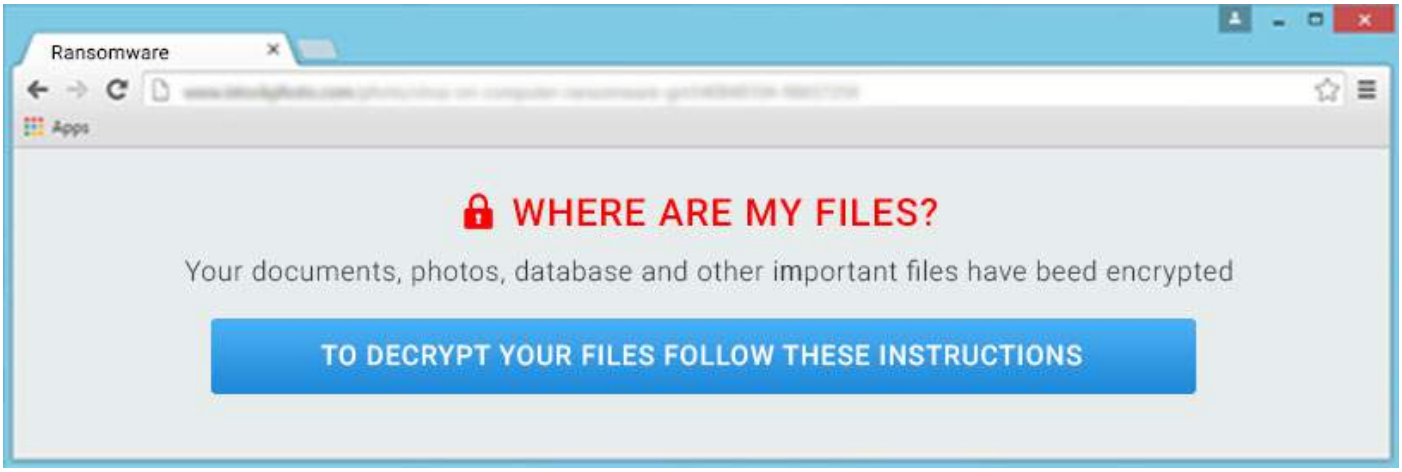
# #3

# Classic Ransomware Behavior


Crypto Ransomware 12

Locker / Lock-Screen Ransomware 13

Fake AVs 13




*An example of a ransom note that is sent to the victim, which includes a link to a hidden Tor website*

# Crypto Ransomware

Crypto ransomware are variants that encrypt data on an infected host, and demand ransom in exchange for decrypting it. The chain of events in a common crypto ransomware attack is as follows:

**Infection**
The ransomware infects a victim's host via one of the different attack vectors mentioned above, causing the execution of the malware.

**Data Encryption**
Once executed, the ransomware scans selected directories and uses various encryption algorithms to encrypt the targeted file types. While some ransomware variants encrypt only certain volumes or folders, others search for files from all the drive letters on the PC, including removable drives, network shares, and even DropBox mappings or other cloud services. The danger lies in the extent of the infection because the ransomware can reach an entire network and cause extended damage to the organization.

Many attackers use AES[1] (symmetric) and/or RSA[2] (asymmetric) encryption to encrypt the selected files. Sophisticated samples tend to use less common techniques, some combining symmetric and asymmetric encryption algorithms. The encryption keys can be stored on the attackers' server or can be locally generated on the victim's host.

After the encryption, the ransomware usually adds a unique extension to the encrypted files (for example: file.locky). In addition, backup files are removed to prevent the option of restoring the encrypted files (shadow volume copies). Most variants also use numerous persistence mechanisms, such as modifying certain registry keys, in order to cause the automatic launch of the malware at every system boot.

**Ransom Note and Payment**
After seizure of the data, a ransom note is presented, usually with a link to a hidden Tor website, containing payment instructions. Payment is most commonly demanded in Bitcoin, as opposed to more traceable payment methods, such as bank accounts or PayPal.

[1] AES (Advanced Encryption Standard) is a symmetric encryption algorithm. Symmetric encryption algorithms use the same cryptographic keys for both encryption and decryption. AES was designed to be effective in both hardware and software. It supports a block length of 128 bits and key lengths of 128, 192, and 256 bits.

[2] RSA is an asymmetric cryptographic algorithm for encrypting and decrypt messages. Asymmetric algorithms use pairs of keys – in each one of the pairs, one key encrypts data and the other one decrypts it. It also uses public key cryptography where anyone can use the public key to encrypt data, but only the possessor of the private key is able to decrypt it.

## Locker/Lock-Screen Ransomware

Locker ransomware are variants that deny access to the infected host and extort money from the victim in exchange for "releasing" the host.

Most ransomware families of this kind "lock" the device by constantly bringing the ransom window to the foreground in an infinite loop, demanding ransom in order to "unlock" the device.

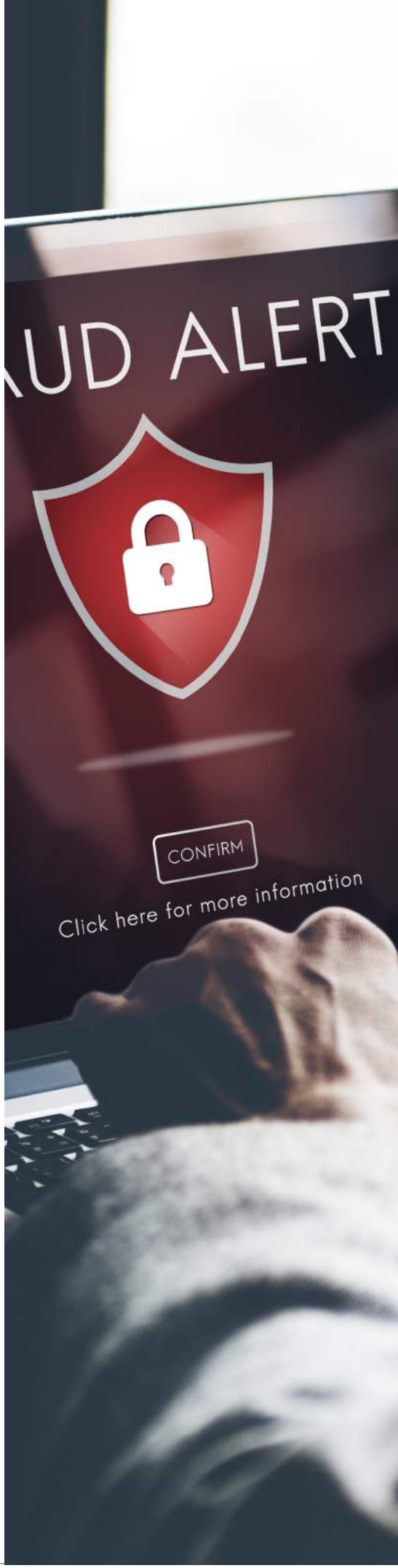
Some variants of this kind present "police themed" messages, which contain a fake warning by an alleged enforcement agency, falsely claiming that the system has been used for illegal activities or is using an illegal version of Microsoft Windows, demanding ransom to unlock it and avoid "legal consequences".

## Fake AVs (Rogue Security Software)

Rogue Security Software are programs that warn the user against malware that has allegedly infected the device in an attempt to convince (and sometimes even force) the user to purchase a security software, in order to "remove" the alleged malware. Moreover, rogue security software often copies the design and names of well-known security programs.

While the common attack vectors for this type of ransomware are the same as the ones mentioned in the introduction, another major attack vector is social engineering: getting victims to believe their device is infected with malware, and manipulating them to download the rogue security software in order to remove it. This type of ransomware might display a scanner on the infected device's screen, pretending to scan the device. Once the "scan" is complete the victim is shown a large number of malware infections that were supposedly found on their device.

Eventually, their purpose is making a profit – they either convince the victim that their device is at risk or basically behave as locker ransomware, denying the use of the programs on the victim's device, while displaying security alerts, until they leave no choice other than purchasing the service (i.e. paying the ransom in order to "unlock" the victim's device).



# #4

# Unique Ransom Behavior

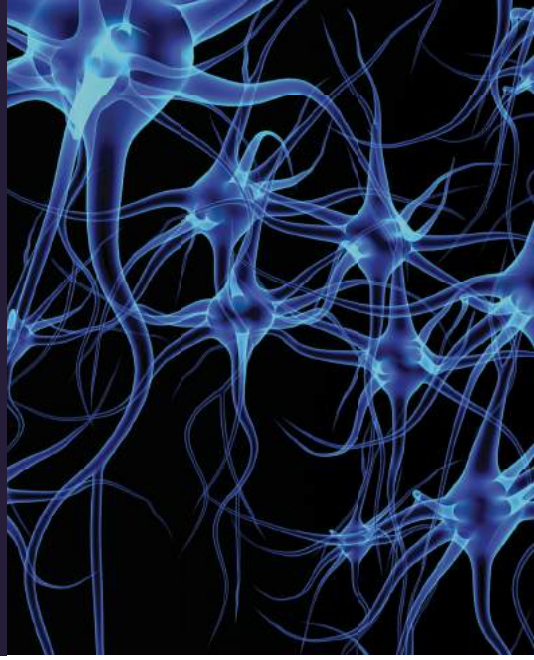

Attack Vectors 15

Encryption Methods 16

C&C Communication 16

Evasion Techniques 17

Ransomware continues to pose a significant threat as new variants keep evolving, presenting more sophisticated capabilities. In the course of our research, we came across a few more sophisticated, novel variants that incorporate new attack vectors, evasion techniques, targeted platforms, and more. These “unique” ransomware are set out below.



# Attack Vectors

The attack vectors of these specialized ransomware families are as diverse as their “classic” counterparts, with most of them sharing the same attack vectors mentioned in the previous section.

The following are more extraordinary methods which are utilized by very few ransomware families:

| Ransomware Name | Unique features |
|---|---|
| **LaChiffre, LowLevel04, and Bucbi** | These ransomware families brute force weak passwords on computers running RDP (Remote Desktop Protocol). Bucbi even uses a brute force utility named “RDP Brute”, and targets corporate networks. |
| **Samas /MIKOPONI (recently hit MedStar Health in the US)** | Uses exploits on open source server platforms (such as JexBoss) to install itself in targeted web servers, and PSExec (executes programs on remote systems with high privileges) for endpoint proliferation within the network. |
| **Surprise** | The first ransomware to attack via TeamViewer. |
| **CTB-Locker** | Uses an affiliate program for distribution (outsources the infection process to a network of affiliates or partners, in exchange for a cut of the profits). As a result, it facilitates a wide range of attack vectors, such as spam campaigns, exploits (via exploit kits including Rig and Nuclear), etc. |
| **Operation Global III** | Changes the encrypted files’ extensions to .exe, and infects them with malicious code that allows the files to spread to other computers once the files are opened. It also looks for unmounted network shares and mounts them as a drive letter on the infected computer. It then proceeds to encrypt and infect the files found on these network shares as well. |

# Encryption Methods

The following are unusual encryption methods that have been observed in these unique families:

| Ransomware Name | Unique features |
|---|---|
| **KeyBTC** | Uses the open source GnuPG program, to create encrypted copies of the user's files, and SDelete from SysInternals to delete the originals, making them unrecoverable. |
| **Petya** | This ransomware overwrites the victim's MBR (Master Boot Record), so that Windows cannot be loaded. Only the "ransom note" is accessible to the victim, providing payment instructions. |
| **CryptoHost** | This ransomware moves files into a password-protected RAR archive. |
| **Rokku** | This ransomware encrypts each file with its own unique key. |
| **RAA** | A JavaScript ransomware that encrypts files using code from CryptoJS, an open source library. |
| **CTB-Locker** | An acronym for Curve-Tor-Bitcoin, also known as Critroni. It uses elliptic curve cryptography: a public key encryption method, which generates keys based on the elliptic curve theory. The generated keys are smaller compared to traditional methods. |
| **CTB-Locker WEB** | This ransomware only targets and encrypts websites. |
| **Jigsaw** | Instead of encrypting, this ransomware steals copies of all the user's files, and deletes the original ones (along with their backups). |

# C&C Communication

Even though Tor is popular among attackers, we have encountered several creative means of C&C communication:

| Ransomware Name | Communication with C&C |
|---|---|
| **Chimera** | This ransomware communicates over Bitmessage, a peer-to-peer messaging application. |
| **Vipasana** | This ransomware does not communicate with a C&C server, but encrypts offline, without any key exchange between the infected device and the attacker. |
| **Bucbi** | This ransomware is fully controlled only via RDP. |
| **TorrentLocker** | This ransomware communicates using HTTPS POST requests. |

# Evasion Techniques

In the course of our research, we came across a few interesting techniques that ransomware variants utilize to bypass security programs and avoid their detection and analysis:

| Ransomware Name | Unique features |
|---|---|
| **Surprise** | This seemingly benign executable dynamically loads another encrypted PE that contains the malicious functionality. |
| **PowerWare** | An open-source PowerShell ransomware that is file-less: all malicious actions are performed via PowerShell commands. No files are saved in the victim's hard drive. |
| **TeslaCrypt 4.1A** | This ransomware shuts down the Task Manager / Process Explorer from SysInternals. It also prevents the execution of the Registry Editor, the command prompt, and msconfig. |
| **CTB-Locker** | This ransomware uses executables that have been signed with a stolen certificate (some AVs automatically skip signed files without scanning them). |
| **CryptXXX** | This ransomware waits 62 minutes before executing any malicious activity, in order to avoid virtual execution detection. |
| **Ransom32** | This JavaScript ransomware is distributed as a self extracting WinRAR archive. It drops and executes the extracted payload: chrome.exe – a fake chrome browser which runs a malicious Node JS application. |
| **LaChiffre** | This ransomware drops a copy of itself, disguised as a jpg, in the victim's Recycle Bin. |
| **Scraper (TorLocker)** | This ransomware is packed with UPX (an open source executable packer), along with the KazyLoader and KazyRootkit protectors. KazyLoader is a .NET two-stage protector of executable files, which encrypts the executable's content in several stages. The KazyRootkit is a .NET protector as well. It presents the following evasion techniques: it hides processes and registry keys from the task manager and the registry editor. This ransomware is also capable of detecting security tools (Wireshark, Sandboxie, etc.), consequently shutting down without unpacking the executable (i.e. activating its malicious functionality). |

# #5 Trends and Forecast


Data Wipers 19

From B2C to BTB: Hospitals, Banks and Industrial Institutes 20

File-less Ransomware Infections (Including Scripts) 21

MBR Overwriters 22

RaaS: Ransomware-as-a-Service 22

EDA 2 / HiddenTear 23

Mobile Ransomware 24

Hybrid Ransomware (Including IoT) 27

Data Collection Instead of Data Encryption 27

The ransomware developers' community keeps evolving, given the fact that the business is profitable – as long as people keep paying ransom to the attackers their efforts pay off. We come across new ransomware campaigns every few days, and it seems they're here to stay. However, the attackers will not necessarily continue spreading the typical types of ransomware (such as the well-known Cerber or CryptoWall) – we are starting to see new trends in the market, set out in this section.

# Data Wipers

We might see an increase in data wipers ransom variants instead of Crypto ransomware. Data wiping means rendering all data on a hard drive unreadable, most commonly by using hard drive over-writers.

An example of a data wiping ransomware, rather than just an encrypting one, is Jigsaw ransomware, which steals copies of all the user's files, and deletes the original ones (along with their backups). FairWare is yet another "wiping" ransomware variant, which deletes web files from Linux servers.

As such, we might see more attackers demanding ransom for recovering "wiped" data, rather than encrypted data. This method is much more destructive because when dealing with Crypto ransomware, when there are errors in the encryption process, the data held ransom can be salvaged without paying ransom by using decryptors that are available online (assuming file recovery is not an option in both cases, that is if the attackers did a good enough job). In contrast, "wiped" data cannot be restored.

# From B2C to BTB: Hospitals, Banks and Industrial Institutes

So far, the vast majority of ransomware families targeted end-users rather than organizations. The exponential growth in the scale of attacks is just the first step towards larger, more lucrative attacks, as seen in the well-known attacks on US hospitals – the Methodist Hospital in Henderson and the Hollywood Presbyterian Medical Center, which were both hit by Locky, and MedStar Health, which was hit by Samas (also known as MIKOPONI). Samas ransomware uses exploits on JexBoss (an open source server platform) to install itself in targeted web servers. It then proceeds to the next stage of network acquisition and mapping, with the aim of proliferating within the network and infecting more end-points. Eventually the attackers use PSExec (executes programs on remote systems) to infect those endpoints.

But hospitals aren't the only "compliant" victim paying the attackers. There has been a concerning increase in both the number and severity of attacks against financial institutions involving ransom demands reaching up to $5,000 each. The LeChiffre ransomware, hit Indian banks, among other targets. Banks are an appealing target - the notorious online banking fraud cybercriminals responsible for the Dridex Trojan have recently added ransomware to their repertoire.

The ransomware Operation Global III is yet another ransomware family which already presents capabilities of proliferation within networks: once it has been executed and has completed encrypting files, it changes their extensions to .exe and infects them with malicious code that allows them to spread to other computers once the files are opened. It also looks for unmounted network shares and mounts them as a drive letter on the infected computer. It then proceeds to encrypt and infect the files found on these network shares as well.

Corporate networks are not the only ones at risk. The next step towards a severe ransomware attack is when ransomware targets industrial networks, not necessarily by encrypting files, but simply by disrupting activity, which could cause electric, water, gas, or nuclear utilities to shut down until the ransom is paid. In April 2016 BWL – the third-largest electric and water utility in Michigan - was under a ransomware attack, and so was the first electric utility hit by ransomware. The attack occurred after an employee opened a malicious attachment. In this case, only the corporate network was infected and no damage has been done to the water or energy supplies. However, any future attacks on such companies could be much more destructive.

We expect to continue seeing the development of more variants such as the ones mentioned above, that will specifically target enterprises, since they are more likely to pay large amounts of money, in comparison to private users. Furthermore, since businesses do not want to risk having the attack become known to the public, affecting their reputation, or to disrupt their operations, they are driven to pay the ransom.

Ransomware families targeting enterprises are likely to be "multi-variants" (i.e., have different variants for each OS), or even cross-platform (such as JavaScript ransomware – please see section on: File-less Ransomware Infections). Locky, for instance, infects Windows, OS X and Linux. KeRanger targets OS X, but it might actually be a rewrite of Linux.Encoder, which targets Linux web servers. And yet, the vast majority of current families targets only Windows. However, cross-platform / "multi-variants" ransomware could hit every server, client, mobile device, or any other network component, and even industrial components (such as SCADA) in the organization, leaving no uninfected end-point, and no recoverable backups.

# File-less Ransomware Infections (Including Scripts)

Targeted attacks on corporate networks, in which the attackers aim to infect every platform within the network, do not necessarily require writing compatible file-based malware for each of these platforms. Instead, by simply using compatible vulnerabilities / hacking / networking tools, attackers can seize every end point. Consequently, attackers can perform more file-less infections[3] to evade detection.

Such attacks can be performed by hacking into organizations, escalating privileges, and proliferating throughout the network without actual file-based malware. Alternatively, attackers can use legitimate networking tools, such as IT, administration, remote desktop, FTP, SSH and Telnet tools. Even TeamViewer was already abused by Surprise ransomware in order to infect computers. The data encryption / wiping can also be committed by using shell commands, for example, PowerWare ransomware is a file-less PowerShell variant that encrypts the victim's data using only PowerShell commands.

Other file-less infection techniques that attackers can take advantage of are using WMI remotely, Windows Registry malware or memory resident malware (loads malicious code to the memory space of a host process, e.g. reflective DLL injection).

An obvious downside of file-less malware infections is the struggle to maintain persistence, in comparison to classic malware, which can easily gain persistence using more simple and common methods. Nevertheless, unlike APT campaigns, ransomware attacks do not necessarily require persistence (apart from locker ransomware and fake AVs). Most ransomware types simply require running once, and encrypting or wiping the user's data without being detected and blocked. Consequently, ransomware attackers are likely to give up persistence in the favor of evasion, i.e. give up file-based infections in favor of file-less infections.

**"Executables-less" Infections using Scripts**

Scripts are another form of file-less, or "executable-less" infections, which is becoming popular, particularly JavaScript ransomware. We came across a few families of such kind:

- **RAA:** A JavaScript ransomware that encrypts files using code from CryptoJS, an open source library.
- **Ransom32:** This JavaScript ransomware is distributed as a self extracting WinRAR archive. It drops and executes the extracted payload: chrome.exe – a fake chrome browser which runs a malicious Node JS application.
- **XRTN:** This JavaScript ransomware is part of the well-known VaultCrypt family.

An additional attempt to evade detection using scripts was recently made by Locky and Cerber, which used a WSF (Windows Scripting File) dropper. WSFs are files that can contain scripts from any Windows Script compatible scripting engine (VBScript, JavaScript, etc.). However, many security solutions do not support WSF detection, enabling attackers to leverage them for ransomware attacks.

[3] No files are saved in the victim's hard drive, which makes it harder for AVs to scan and detect the ransomware, thus evading static analysis.

# MBR Overwriters

We expect to encounter more ransomware variants that deny access to the infected host and its entire operating system, rather than just to certain files. “MBR Overwriters” prevent the operating system from booting by overwriting the MBR (Master Boot Record). The consequences are similar to those caused by locker ransomware, but the mode of operation is more sophisticated than the methods used by classic "lock-screen" variants that are currently seen in the wild.

The technique has been used in the well-known Sony Attack, and as such, we have already observed a ransomware variant that used this destructive method: Petya ransomware overwrites the victim’s MBR so that Windows cannot be loaded. Instead, only the “ransom note” with payment instructions is accessible to the victim. This ransomware has recently become publicly available as a Service, or RaaS, as set out below.

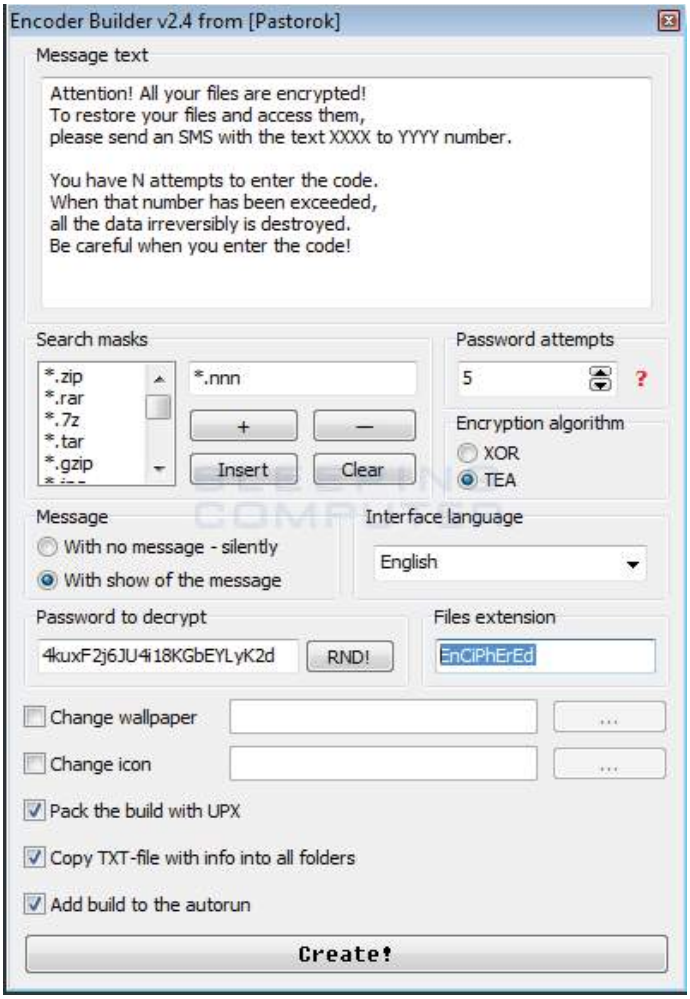
# RaaS: Ransomware-as-a-Service

Much has been written regarding the growing sophistication of the cybercrime industry, which has adopted a corporate nature. Ransomware-as-a-service (RaaS) fits into the new nature of Crime-as-a-Service (CaaS), incorporating a classic “affiliate” distribution model where malware creators sell their product to clients who distribute it in their private, profitable ransomware campaigns. In RaaS, the ransomware distributor acts as an affiliate, paying the ransomware creator a small cut of the profits, somewhere between 5 and 25 percent. By using anonymous Bitcoin addresses and the Tor network, the creator and distributor can remain anonymous, keeping a safe distance from law-enforcement authorities.

Ready-to-use ransomware can also be purchased as a kit on the Dark Web, and be personally configured via simple GUIs enabling the customization of many parameters such as attack vectors, encrypted file types, encrypted file extensions, the content of the ransom note, and more.

Anyone can become a distributer, as can be seen by RaaS Encryptor, which is a ransomware advertised on an onion-based domain via Tor2Web service, as well as the Petya and Mischa ransomware that are available on the market as RaaS.

A clear prototype of this trend is the Xorist ransomware builder, which can also be purchased from the Dark Web and exploit forums. It can be very easily configured, not necessarily requiring the skills of an experienced attacker. Below is an example:




*An example of a ransomware builder that can be purchased on the Dark web*

# EDA2 / HiddenTear

A Turkish programmer named Utku Sen created open-source ransomware HiddenTear and EDA2 as a proof-of-concept for educational purposes. He uploaded them onto GitHub on August 2015, indirectly making them publicly available to attackers. Any attacker with basic programing skills can use the code to create a ransom campaign of his own, as had happened. Open-source ransomware of such kind is a major threat, because similar to the RaaS phenomenon, they create opportunities for unexperienced attackers to distribute their own ransomware campaigns with minimal effort.

# Known Families Based on These Projects

**Known Families Based on EDA2:**

- Surprise: a ransomware installed via TeamViewer that executes a modified EDA2 ransomware variant.
- Brazilian
- Magic
- Strictor
- MM Locker
- SkidLocker/Pompous

**Known Families Based on HiddenTear:**

- Hi Buddy
- Job Crypter
- KryptoLocker
- MireWare
- Rush/Sanction
- Fakben

The disadvantage of EDA2 and HiddenTear is that due to their popularity among attackers, most endpoint protection solutions have developed static signatures that detect and block them. Therefore, we believe that their prevalence is about to decrease. However, due to the availability of similar "ready-to-use" ransomware infrastructures among attackers, creating opportunities for them, the number of attacks is likely to increase. Stampado ransomware, for instance, is being sold to attackers on the Dark Web for only $39. An industry in which any unexperienced attacker can become a distributer and make profits out of major campaigns has the means to evolve quickly.

# Mobile Ransomware

The ransomware industry hasn't limited itself to PCs, extending its reach to attack mobile devices. Android is found to be the operating system that is more prone to ransomware attacks – with a 5.7% risk of malware compared to 3.0% in iOS, due to a greater variety of Android ransomware attacking Android-OS smartphones. In 2014, Simplocker, the first mobile Crypto ransomware, started spreading. It encrypted data (images, documents, videos) using AES (Advanced Encryption Standard).

Locking / lock-screen ransomware and fake AVs are quite common in the mobile ransomware industry as well. However, a different type of mobile ransomware threat is also accelerating – extortion ransomware. These ransomware families threat to embarrass victims by exposing to their entire contact list: private photos, subscriptions to porn services (real / fake), etc.

Most victims get infected with mobile ransomware as a result of targeted (spear phishing) /non-targeted (phishing) attacks or by willingly installing malicious apps from other sources than Google Play/App Store (malicious websites for instance), as a result of social engineering.

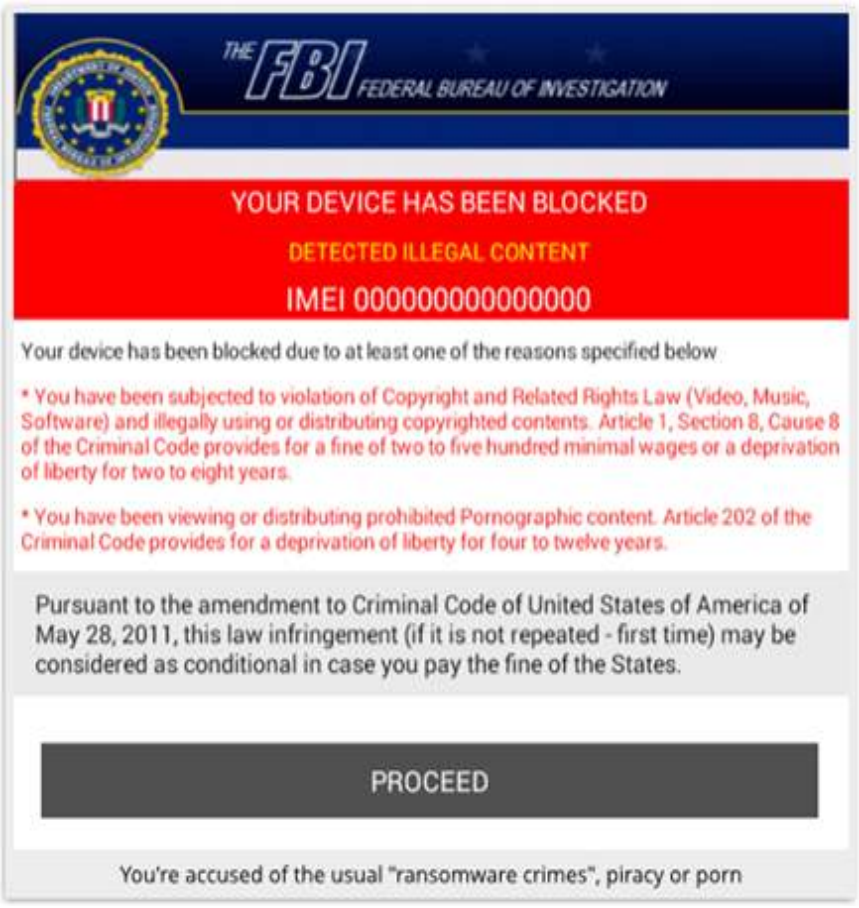
According to AVAST: there was a 5-6% year-to-year growth of mobile ransomware infections, between the beginning of 2015 and the beginning of 2016.

# Interesting Mobile Ransomware Variants

### Locking Mobile Ransomware

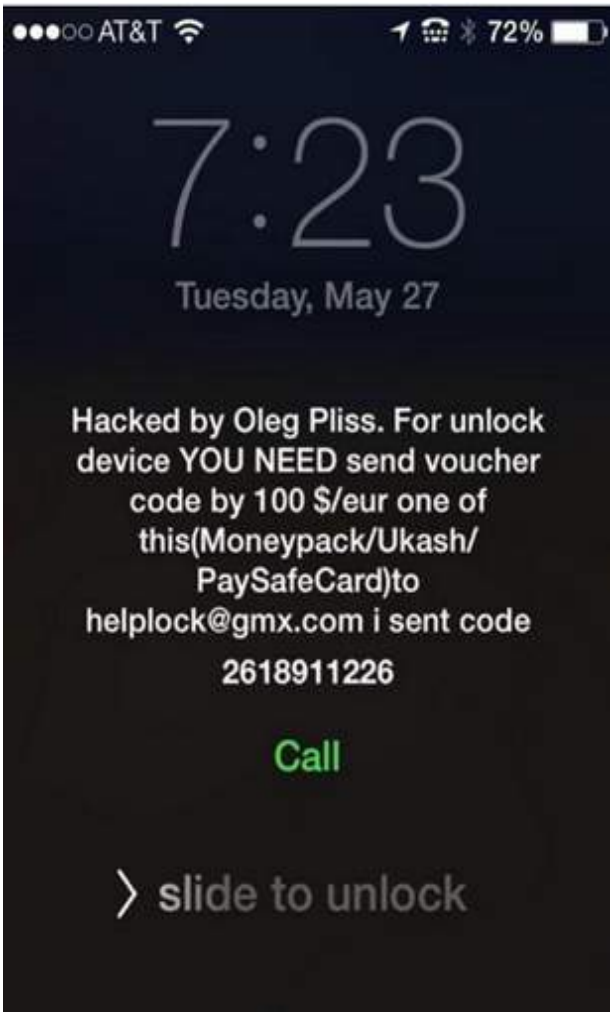
This type of ransomware denies access to the device. The first ransomware family of this type "locked" the device by constantly bringing the ransom window to the foreground in an infinite loop. Nowadays, we are exposed to more complex methods:

| Ransomware Name | Description |
|---|---|
| **LockerPin** | An Android ransomware that tries to gain device administrator privileges in order to set the phone's PIN lock. (It's important to note that the forthcoming version of Android - dubbed Nougat, will prevent this method; device admins will no longer be able to clear passwords or change ones that are already set). |
| **ScarePakage** | An Android ransomware that kills every running process (other than the malware itself) after 10 milliseconds (by using a Java TimerTask). It also prevents the device from going into sleep mode (using an Android WakeLock). |
| **FBI Locker** | An Android ransomware that is disguised as a fake Flash Player application. Once executed, it presents the following fake FBI alert. |




*An example of a ransomware note that demands ransom in order to unlock the device and "avoid other legal consequences"*
*Source: https://nakedsecurity.sophos.com/2014/07/25/android-fbi-lock-malware-how-to-avoid-paying-the-ransom/*

| Ransomware Name | Description |
|---|---|
| **iCloud locker ransomware** | A recent iOS ransomware variant that abused the "Find My iPhone" app for its distribution. The attacker broke into victims' iCloud accounts and activated the app on their devices, setting the device into "Lost Mode", which allows users to block access to the device and enter a message on its screen. The attacker used this feature to present its ransom message. |




*An example of a ransomware note on a mobile device*
*Source: [http://securitywatch.pcmag.com/security/324170-ransomware-on-apple-s-icloud-how-the-attack-worked](http://securitywatch.pcmag.com/security/324170-ransomware-on-apple-s-icloud-how-the-attack-worked)*

### Extortion Mobile Ransomware

This type of ransomware threatens to embarrass victims by exposing to their entire contact list data such as private photos, subscriptions to porn services (real / fake), etc. Ackposts, for instance, is an Android ransomware that is distributed in the Japanese market (disguised as a legitimate app). It creates fake subscriptions to porn services, and threatens the victim to broadcast them to its entire contact list, unless the ransom is paid.

# Hybrid Ransomware (Including IoT)

We expect that the ransomware industry will continue to develop and produce more aggressive variants, in order to maximize profits; combinations of ransomware possessing banking Trojans' capabilities[4], along with worms' spreading methods[5] , could produce much more profitable variants. Such "hybrid" ransomware families are already seen in the wild; The Android Trojan Xbot is not only a ransomware, but also a banking Trojan. It combines information stealing, intercepting SMS messages, remotely locking the device and encrypting data.

Accessing IoT is yet another capability future ransomware may possess; In the last DefCon, the security firm Pen Test Partners demonstrated creating a PoC (Proof-of-Concept) ransomware for a smart thermostat. Such ransomware could set extreme temperatures, waste vast amounts of power, and even cause physical damage, unless the ransom is paid.

# Data Collection Instead of Data Encryption

We might start seeing ransomware focusing on data collection rather than data encryption. Attackers might stop using the tactics of encrypting files, and simply steal important or confidential data from private users, and even more likely from businesses, and extort payment in return for not distributing the data. This approach is already used by many mobile ransomware variants (please see the section on Extortion Mobile Ransomware), however, it might get popular among PC variants as well. Chimera ransomware, for instance, already uses such a tactic of threatening to publish the victim's files unless the ransom is paid.

[4] Stealing login credentials and intercepting voice/sms communications, in order to gain access to the victim's bank account and gain ability to perform transactions.

[5] Spreading independently over end points, in very large scales, by exploiting operating system vulnerabilities / spreading spam emails / SMS messages.

# #6

# Conclusion: Steps to Avoid Becoming a Ransomware Victim


What is the Extent of the Damage that Can Happen to Your Organization from Ransomware? 29

How Can You Avoid Falling Victim to Ransomware? 29

Your Organization is Already Infected, What Can You Do? 30

Should Your Organization Just Pay the Ransomware? 31

What Should You Do if Your Organization Has Paid the Ransomware? 32

# What is the Extent of the Damage that Can Happen to Your Organization from Ransomware?

The main damage is disruption of operations because you will not be able to use your devices to access files, apps or even the entire operating system. The ransomware attack on the Hollywood Presbyterian Medical Center's computer system in Los Angeles, caused the hospital to return to faxes and paper charts.
Data leaks are yet another potential risk, in case the attacker threatens to publish the encrypted / wiped data, unless the ransom is paid.

# How Can You Avoid Falling Victim to Ransomware?

**Personal diligence:**

- Make sure all your files are backed up on an external device.
- Do not open suspicious links that were received from emails or social media channels, such as: Twitter, Facebook, etc.
- Do not open suspicious emails and particularly email attachments. According to PhishMe, at the end of March 2016, 93% of all phishing emails contained Crypto ransomware (compared to 56% in December 2015 – a major increase).
- When you open attachments that contain Offices documents, do not automatically click "enable macros"[6] . Many malware families are distributed in Office documents which trick users into enabling macros, allowing the malware to execute itself. Microsoft deliberately turned off auto-execution of macros by default many years ago as a security measure. According to Microsoft, 98% of Office-targeted threats use macros. To avoid the risk, only enable macros from trusted sources, and use the Microsoft "Block macros from running in Office files from the internet" option, so that users won't be able to enable macros from any Office files that were downloaded from the Internet.
- Some malicious scripts, which require executing outside of the browser, rely on Windows Script Host. We recommend disabling it, preventing any scripts (including VBScript and JScript) that rely on it from running.
- Use an anti-spam service.
- Keep your operating system and other programs up-to-date to avoid attackers exploiting vulnerabilities.
- Block TOR in your network – many ransomware variants use TOR proxy servers.
- Use end-point security solutions.

[6] Macros are embedded code written in a programming language known as Visual Basic for Applications (VBA), which can ease automation of repetitive tasks. Microsoft Office documents — Word, Excel, PowerPoint, and other types of documents — can contain macros. Source: http://www.howtogeek.com/171993/macros-explained-why-microsoft-office-files-can-be-dangerous/

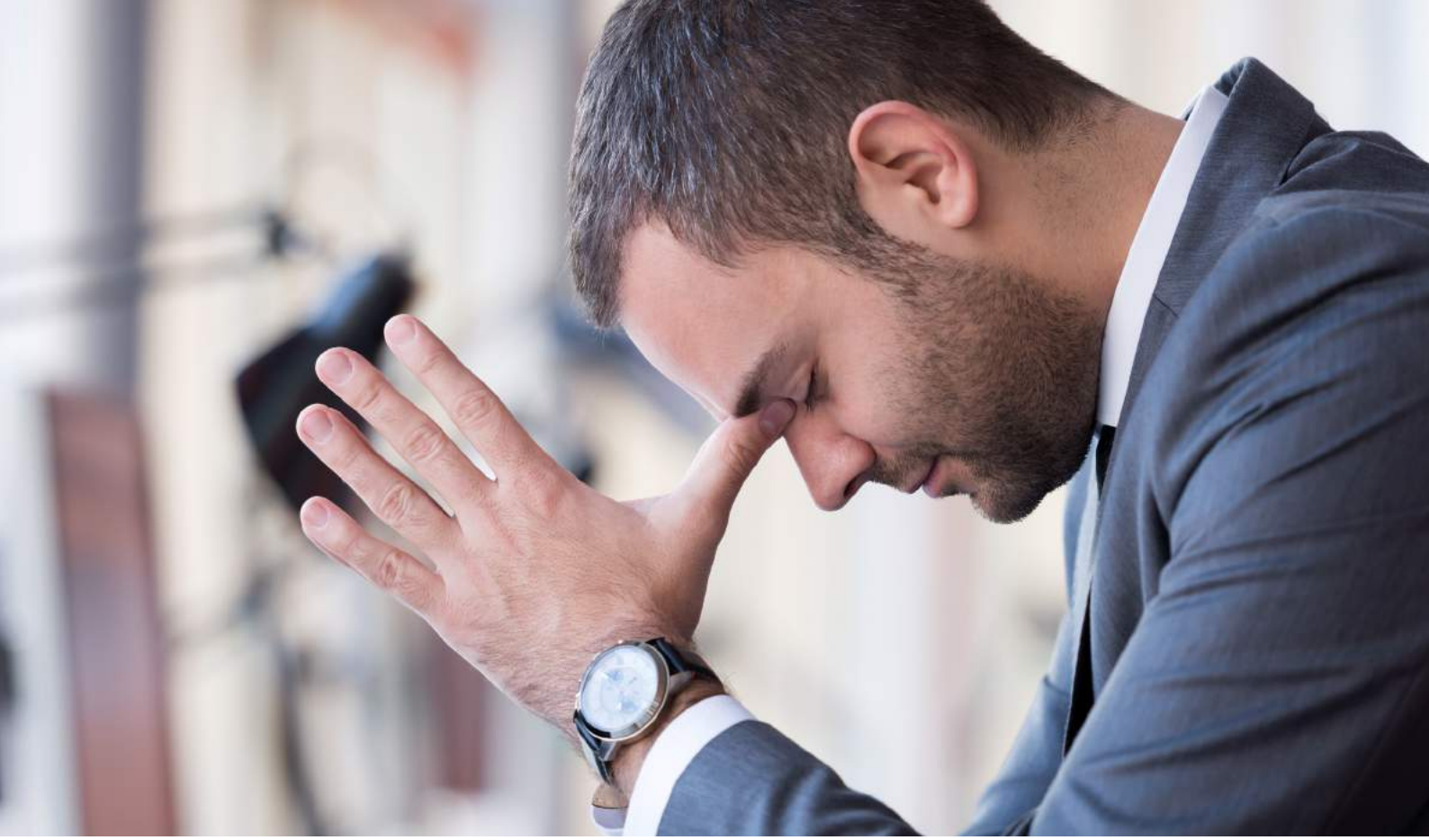

**Organizational Diligence:**

- Train your employees to maintain a secure routine, which includes the above mentioned steps.
- Install endpoint and email protection solutions and a reliable security suite offering multiple layers of protection.
- Manage users' privileges and access. Avoid providing users with access to important directories when it is not necessarily required, particularly administrative access (could be easily configured in Windows, using GPOs[7] in domains, and LGPOs (local GPOs) in workgroups).
- Implement a mandatory backup policy.
- Create a centralized patch management system for Microsoft Office, Adobe applications, web browsers, and browser plug-ins to minimize exploits.
- Have an emergency response plan in place.
- Enforce secure browser settings.
- Use a combination of strategies (i.e. ensure backups in different platforms) to have a 'Plan B' in place, in the event that a certain backup on a certain platform has been infected. This could include a recovery tool that can be accessed from a strategically placed server.

# Your Organization is Already Infected, What Can You Do?

- If you noticed the infection before the ransom note appeared, you should shut down your device immediately and disconnect it from the network. There's a chance the malware didn't finish encrypting the files, uploading them to its C&C server, or deleting shadow volume copies (in which case you would be able to restore your data).
- Look online for a decryptor on another device, since many ransomware families deny access to the browser. Browlock, for instance, is a police themed ransomware that blocks access to the Internet. It uses the browser to display a lock screen demanding the victim to pay a fake fine and plays tricks to prevent closing the browser tab.
- Verify that the decryptor is legit, by submitting it to a file scanning service, such as VirusTotal. We have also seen ransomware being distributed as a file restore program, for example, the Rector ransomware is distributed under the name of 'RectorDecryptor' - a program which allegedly helps users recover their lost files.
- Alert the authorities – there might be a way to reach the attacker and get your data back, without paying.
- Most importantly, avoid paying. Paying the attackers is what keeps them going. As long as the industry is profitable, the rate of this type of cyber-attacks will continue to increase.

[7] GPO – Group Policy is an infrastructure that allows you to implement specific configurations for users and computers.
Source: https://technet.microsoft.com/en-us/windowsserver/bb310732.aspx



# Should Your Organization Just Pay the Ransomware?

Avoid paying at all costs. By paying the attackers, you only contribute to the profitability and long term sustainability of this criminal source of income. Furthermore, the FBI issued an advisory strongly advising not to pay the ransom since it "doesn't guarantee an organization that it will get its data back—we've seen cases where organizations never got a decryption key after having paid the ransom. Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. And finally, by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals." This nightmare scenario was experienced by Kansas Heart Hospital, which was hit with a ransomware attack. After the hospital paid the ransom, the attackers tried to extort a second payment.

# What Should You Do if Your Organization Has Paid the Ransomware?

You should contact your bank, your local and federal law enforcement authorities, as well as communication authorities.

Certain countries have governmental fraud and scam reporting websites:

| Country | Fraud and Scam Reporting Website |
|---|---|
| **Australia** | SCAMwatch |
| **Canada** | Canadian Anti-Fraud Centre |
| **France** | Agence nationale de la sécurité des systèmes d'information |
| **Germany** | Bundesamt für Sicherheit in der Informationstechnik |
| **Ireland** | An Garda Síochána |
| **New Zealand** | Consumer Affairs Scams |
| **United Kingdom** | Action Fraud |
| **United States** | On Guard Online |

# #7
# References

Cyber Security Intelligence (2016, July 22). Ransomware Victims Run into Millions. Retrieved from https://www.cybersecurityintelligence.com/blog/ransomware-victims-run-into-millions--1496.html

CNN Money (2016, April 15). Cyber-extortion losses skyrocket, says FBI. Retrieved from http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/

BBC News (2016, 7 July). Criminals winning 'cyber arms race' - National Crime Agency. Retrieved from http://www.bbc.com/news/uk-36731694

Kaspersky Lab (2016, June 22). PC ransomware in 2014-2016, The evolution of the threat and its future. Retrieved from Securelist https://securelist.com/analysis/publications/75145/pc-ransomware-in-2014-2016/

Infosec Institute (2016, June 8). Ransomware: A Highly-Profitable Evolving Threat. Retrieved from http://resources.infosecinstitute.com/ransomware-an-evolving-threat-even-more-profitable/

msft-mmpc (2016, May 18). The 5Ws and 1H of Ransomware. Retrieved from Microsoft Malware Protection Center, Threat Research & Response Blog https://blogs.technet.microsoft.com/mmpc/2016/05/18/the-5ws-and-1h-of-ransomware/

Microsoft Malware Protection Center. Ransomware. Retrieved from https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx#what

Lawrence Abrams (2015 November 3). CryptoWall 4.0 released with new Features such as Encrypted File Names. Retrieved from Bleeping Computer http://www.bleepingcomputer.com/news/security/cryptowall-4-0-released-with-new-features-such-as-encrypted-file-names/

Phil Muncaster (2016, March 14). UK Enterprises in Trouble as Ransomware Spikes in February. Infosecurity Magazine. Retrieved from http://www.infosecurity-magazine.com/news/uk-enterprises-trouble-ransomware/

Nick Biasini (2015, October 6). Threat Spotlight: CISCO TALOS Thwarts Access to Massive International Exploit Kit Generating $60M Annually from Ransomware Alone. Retrieved from Talos http://www.talosintelligence.com/angler-exposed/

Dhruval Gandhi (2016, April 28). Teepr.com: Yet Another Top Alexa Site Spreading Ransomware. Retrieved from Cyphort Labs Blog http://www.cyphort.com/teepr-com-yet-another-top-alexa-site-spreading-ransomware/

Scott Kosciuk (2016, May 24). 10 shocking malware and ransomware statistics.... Retrieved from Clearswift blog https://www.clearswift.com/blog/2016/05/24/10-shocking-malware-and-ransomware-statistics

Steve Ragan (2016, March 28). Ransomware attack hits MedStar Health, network offline. CSO Retrieved from http://www.csoonline.com/article/3048825/security/ransomware-attack-hits-medstar-health-network-offline.html

CWZ (2016, May 14). Ransomware decryption tools – All the tools you need to get your files back. Cyber War Zone. Retrieved from http://cyberwarzone.com/ransomware-decryption-tools-tools-need-get-files-back-20-decryption-tools/

Brian Krebbs (2016, March 22). Hospital Declares 'Internal State of Emergency' After Ransomware Infection. Retrieved from Krebbs on Security http://krebsonsecurity.com/2016/03/hospital-declares-internet-state-of-emergency-after-ransomware-infection/

Steve Ragan (2016, February 14). Ransomware takes Hollywood hospital offline, $3.6M demanded by attackers. CSO. Retrieved from http://www.csoonline.com/article/3033160/security/ransomware-takes-hollywood-hospital-offline-36m-demanded-by-attackers.html

Tara Seals (2016, January 11). Feds Warn Banks of Rising Ransomware Tide. Infosecurity Magazine. Retrieved from http://www.infosecurity-magazine.com/news/feds-warn-banks-of-rising/

Security Week News (2016, January 26). LeChiffre Ransomware Hits Indian Banks, Pharma Company. SecurityWeek News. Retrieved from http://www.securityweek.com/lechiffre-ransomware-hits-indian-banks-pharma-company

Crosman Penny (2016, March 17). Bank-Hacking Gang Dridex Ramps Up, Branches into Ransomware. American Banker. Retrieved from http://www.americanbanker.com/news/bank-technology/bank-hacking-gang-dridex-ramps-up-branches-into-ransomware-1079972-1.html

Tweet by Lansing BWL @BWLComm at 9:55 AM on 25 Apr 2016 https://twitter.com/BWLComm
Bogdan Botezatu (2016, March 8). KeRanger Is Actually a Rewrite of Linux.Encoder. Retrieved from Bitdefender Labs https://labs.bitdefender.com/2016/03/keranger-is-actually-a-rewrite-of-linux-encoder/

Trend Micro (2016, August 14). New Locky Ransomware Spotted in the Brazilian Underground Market, Uses Windows Script Files. Retrieved from http://blog.trendmicro.com/trendlabs-security-intelligence/new-locky-ransomware-spotted-in-the-brazilian-underground-market-uses-windows-script-files/

Mike Lennon (2014, December 19). Hackers Used Sophisticated SMB Worm Tool to Attack Sony. Security Week News. Retrieved from http://www.securityweek.com/hackers-used-sophisticated-smb-worm-tool-attack-sony

Lawrence Abrams (2016, July 26) Petya and Mischa Ransomware Affiliate System Publicly Released. Bleeping Computer. Retrieved from: http://www.bleepingcomputer.com/news/security/petya-and-mischa-ransomware-affiliate-system-publicly-released/

Security Week News (2016, April 25). Malicious Insiders Could Tap Ransomware-as-a-Service for Profit. SecurityWeek News. Retrieved from http://www.securityweek.com/malicious-insiders-could-tap-ransomware-service-profit

Tomas Meskauskas (2016, 14 March). Surprise ransomware removal instructions. Retrieved from PCrisk https://www.pcrisk.com/removal-guides/9874-surprise-ransomware
Security Week News (2016, July 14). Lifetime License for Stampado Ransomware: $39. SecurityWeek News. Retrieved from http://www.securityweek.com/lifetime-license-stampado-ransomware-39

SkyCure. (2016). Mobile Threat Intelligence Report Q1 2016. Retrieved from https://www.skycure.com/wp-content/uploads/2016/06/Skycure-Q1-2016-MobileThreatIntelligenceReport.pdf

Stefanie Smith (2016, April 5). The evolution of mobile ransomware. Retrieved from avast! blog https://blog.avast.com/the-evolution-of-mobile-ransomware
Android Developer Console. Behavior Changes. Retrieved from https://developer.android.com/preview/behavior-changes.html

Paul Ducklin (2014, July 25). Android "FBI Lock" malware – how to avoid paying the ransom. Retrieved from Naked Security by Sophos https://nakedsecurity.sophos.com/2014/07/25/android-fbi-lock-malware-how-to-avoid-paying-the-ransom/

Abigail Wang (2014, June 7). Ransomware On Apple's iCloud: How the Attack Worked, SecurityWatch. Retrieved from http://securitywatch.pcmag.com/security/324170-ransomware-on-apple-s-icloud-how-the-attack-worked

Andrew Tierney (2016, August 8). Thermostat Ransomware: a lesson in IoT security. Retrieved from Pen Test Partners https://www.pentestpartners.com/blog/thermostat-ransomware-a-lesson-in-iot-security/

Julia Carrie Wong (2016, February 16). Los Angeles hospital returns to faxes and paper charts after cyberattack, The Guardian. Retrieved from https://www.theguardian.com/us-news/2016/feb/16/los-angeles-hospital-cyberattack-ransomware-data-computers

PhishMe. (2016). Q1 2016 Malware Review. Retrieved from http://phishme.com/phishme-q1-2016-malware-review/

msft-mmpc (2016, March 22). New feature in Office 2016 can block macros and help prevent infection. Retrieved from Microsoft Malware Protection Center, Threat Research & Response Blog https://blogs.technet.microsoft.com/mmpc/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/

msft-mmpc (2016, June 14). Where's the Macro? Malware authors are now using OLE embedding to deliver malicious files. Retrieved from Microsoft Malware Protection Center, Threat Research & Response Blog https://blogs.technet.microsoft.com/mmpc/2016/06/14/wheres-the-macro-malware-author-are-now-using-ole-embedding-to-deliver-malicious-files/

Microsoft TechNet. Disabling Windows Script Host. Retrieved from https://technet.microsoft.com/en-us/library/ee198684.aspx

Chris Hoffman (2013, September 11). Macros Explained: Why Microsoft Office Files Can Be Dangerous. Retrieved from How-To Geek http://www.howtogeek.com/171993/macros-explained-why-microsoft-office-files-can-be-dangerous/

VirusTotal https://www.virustotal.com/

FBI. Gov (2016, April 29). Incidents of Ransomware on the Rise Protect Yourself and Your Organization. Retrieved from https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise

Ms. Smith (2016, May 22). Kansas Heart Hospital hit with ransomware; attackers demand two ransoms. Retrieved from Network World by IDG http://www.networkworld.com/article/3073495/security/kansas-heart-hospital-hit-with-ransomware-paid-but-attackers-demanded-2nd-ransom.html

Microsoft Technet. Windows Server. Retrieved from https://technet.microsoft.com/en-us/windowsserver/bb310732.aspx

# About Deep Instinct

Deep Instinct is the first company to apply deep learning to cybersecurity. Leveraging deep learning's predictive capabilities, Deep Instinct's on-device, proactive solution protects against zero-day threats and APT attacks with unmatched accuracy. Deep Instinct provides comprehensive defense that is designed to protect against the most evasive unknown malware (including ransomware) in real-time, across an organization's endpoints, servers, and mobile devices. Deep learning's capabilities of identifying malware from any data source results in comprehensive protection on any device, any platform, and operating system. Deep Instinct is headquartered in Tel Aviv, Israel and has offices in San Francisco, CA. To learn more, visit: http://www.deepinstinct.com

www.deepinstinct.com

Deep Instinct Ltd.
23 Derech Menahem Begin, Tel Aviv, 66182 Israel +972 (3) 545-6600
501 Folsom Street, Suite 400, San Francisco, CA 94105, USA +1 (855) 522-2223



Deep Instinct has invested significant efforts to make this research as updated as possible. However with the high rate of reports of ransomware attacks, on almost a daily basis, this research fully covers all unique ransomware variants until September 6th, 2016.