RANSOMWARE
A GROWING ENTERPRISE THREAT

A deep dive into ransomware's evolution and why businesses can't afford to ignore it

One of the fastest growing threats in cybersecurity today, ransomware is quickly becoming the favored means for cybercriminals to extract a profit from unsuspecting victims. As ransomware mushrooms with new malware variants and new ways of scamming victims, businesses can no longer afford to discount it as a consumer-only problem. In truth, now that there's an established business case for ransomware profitability, criminal ventures are looking for ways to make even more money off their investment. And that's increasingly going to put large organizations in their crosshairs.

In fact, in the first three months of 2016 alone, law enforcement officials estimate that criminals used ransomware to extort $209 million from businesses and institutions[1]. Clearly, ransomware can cost these organizations dearly if they don't start paying attention to the risks.

How Ransomware works

The principle behind ransomware is devastatingly simple, even if the technical details around new variants grow more complex and sophisticated by the day. The idea is that criminals block access to a system or its data until a certain amount of money is paid by the victim.

Ransomware's blockade can be achieved by encrypting files or folders, hindering system access to the hard drive, or even by

manipulating the master boot record to interrupt the system's boot process. New methods of disrupting users' access crop up regularly, but for the most part, cryptoransomware dominates the field. Some variants encrypt large swaths of user folders, others will specifically target the file types most likely to trigger desperation in users seeking recovery, such as images, spreadsheets or Word documents that might hold a lot of personal or professional value.

Criminals count on individuals and business users becoming so frantic about regaining timely access to data that they'll be willing to shell out a hefty ransom in payment for the encryption key necessary to unlock the data. Traditionally, that ransom has equaled about $300 to $500 for individuals, but the amounts can climb steeply when larger -- or wealthier -- targets come into play.

Today, ransomware is usually distributed through highly targeted phishing emails, social engineering schemes, watering hole attacks or malvertising networks. These distribution mechanisms are frequently delivered by commercial malware kits like Angler and Nuclear, which package up the technological components into a turnkey solution ready to be purchased by any enterprising criminal.

THE FBI ESTIMATES THAT RANSOMWARE WILL NET CRIMINALS $1 BILLION IN 2016 [1]

TYPES of RANSOMWARE

ENCRYPTING RANSOMWARE

In this instance the ransomware systematically encrypts files on the system's hard drive, which becomes difficult to decrypt without paying the ransom for the decryption key. Payment is asked for using BitCoin, MoneyPak, PaySafeCard, Ukash or a prepaid (debit) card.

NON-ENCRYPTING RANSOMWARE

In this instance encryption is not used. Instead, the ransomware employs fairly simple techniques to restrict access to the system and prominently displays a pornographic image, or a scam message from law enforcement and asks users for payment using premium-rate SMS, or using the same methods noted for encrypted ransomware, to receive a code to unlock the machine.

"MANY RANSOMWARE PACKAGES HAVE ADDED MORE ADVANCED **ANTIMALWARE EVASION AND PERSISTENCE TECHNIQUES IN RECENT YEARS."**

While early ransomware was fairly rudimentary, the last few years have seen rapid advancement in both antimalware evasion and persistence techniques across many ransomware packages. We'll dig into some of these technological tactics later in the paper, but suffice it to say they help criminals maintain a firm grasp of the system after infection. Add to that the sheer volume of ransomware variants released in the wild and it soon becomes clear how so many ransomware victims have been infected, even when running completely up-to-date antimalware software. The crooks have picked up the pace with polymorphism, spewing out rapid iterations of slightly altered ransomware variants to overwhelm antivirus researchers working on identification signatures. As a result, traditional endpoint defenses simply haven't been able to keep up with the onslaught.

In addition, the encryption technology used by cryptoransomware creators to make data inaccessible to victims also continues to improve swiftly. While ransomware circa 2006 was using 56 bits with "homebrewed" encryption, today's most advanced versions utilize AES symmetric algorithm and RSA or ECC public-key encryption. In a few isolated instances, security researchers have found weaknesses in certain ransomware variants' encryption techniques, allowing development of "one-off" tools allowing victims of that particular variant to recover files. However, these tools can't crack the underlying encryption used by the ransomware. They've just taken advantage of coding errors or sloppy encryption key management by criminals

POLYMORPHISM - this is a technique wherein the harmful, destructive or intrusive computer software such as a virus, worm, Trojan or spyware constantly changes ("morphs"), making it difficult to detect with antivirus programs and scanners.

in order to create limited-use solutions for victims. Many ransomware families often do make these "rookie" mistakes, but most of the bugs/vulnerabilities are usually addressed quickly after researchers identify them.

Unless an organization deploys a protection that includes features specifically targeting ransomware, once that data has been encrypted, there's no reversing it. Without backups, which themselves are often the first target of ransomware, an organization's only recourse is to pay the extortionists. In fact, cryptoransomware has become so exceptionally effective at holding data hostage that some officials have been overheard recommending that victims pay the ransom in the absence of backups.

WHY SHOULD MATURE IT ORGANIZATIONS CARE?

This leads us to the elephant in the room: Many IT administrators and security staffers still view ransomware as largely a consumer problem. That is primarily because most organizations with even a moderate level of maturity have some sort of backup and recovery plan in place. For such organizations, a natural response to the ransomware threat would be, "Why should we worry about malware that encrypts our data if we can just restore it from our backups?"

Unfortunately, this line of thinking does not take the following important factors into consideration.

"SOME OFFICIALS HAVE RECOMMENDED THAT VICTIMS **PAY THE RANSOM IN THE ABSENCE OF BACKUPS."**

Incomplete Backups

While many organizations do have backup recovery plans in place, the execution of these plans may not be complete enough to cover the exigencies of a ransomware attack. For example, backups of certain endpoints may be incomplete or irregular, particularly in the case of remote workers or BYOD endpoints. Even if the data is not mission critical, its loss or temporary unavailability could greatly impact affected users' productivity. In addition, many newer ransomware variants contain code to attack unmapped network drives and even cloud-based assets that may not be included in backup routines.

Cost and Inconvenience of Data Recovery

Let's face it, many backup and recovery plans are called "disaster recovery plans" because the only time it makes sense to spin up recovery procedures is when a wide-scale disaster hits. Even if the data attacked by ransomware is properly backed up, the cost and complexity of recovering it could lead to the conclusion that it’s cheaper and timelier to just pay the ransom in return for immediate access to the data.

Employees May Pay Ransom Covertly

Whether it is because a big project needs to be completed within a couple of hours, or the employee is too embarrassed to approach IT with the problem, there's a very real threat that an employee could pay the ransom without alerting the organization. In such cases, the employee might bear the cost themselves, or hide it in an expense report as some sort of miscellaneous charge, thus avoiding the hassle of IT intervention.

Ransomware's Deletion of Backups

Increasingly, new ransomware variants are finding ways to target backup files as a part of their attack patterns. The more sophisticated extortionists recognize that they lose an opportunity for strong-arming victims when backups are in play, and they're adding this new tactic as a way to maximize their gains.

The bottom line it is that the surge in ransomware is very much a business problem, both for small and medium-sized business and large enterprises. The aforementioned problems present a strong business case for addressing ransomware head-on, but organizations also need to be aware of other lingering impacts.

A Brief History of RANSOMWARE

A Brief History of Ransomware

Following the evolution of ransomware, from a petty crime to a major economic windfall for global criminal enterprises, underscores why businesses should be deeply concerned about the threat. As the sophistication of these attacks grows, so do the aspirations of the perpetrators, and the larger the target, the bigger the potential reward.

While its explosive growth over the past year may make it seem otherwise, ransomware didn't come out of nowhere. In fact, it has been a money-making venture for over a decade, growing gradually as organized criminals started testing the business case for this particular infection and recognizing its potential as a profit model.

Ransomware first cropped up around 2005 as just one subcategory of the overall class of scareware that includes fake AV and phony computer-cleaning utilities.

While it showed some promise early on, it took a few changes in technical and economic conditions before the pump was truly primed for peak ransomware profit. First of all, the early methods used by the criminals to obfuscate or block access to data were fairly rudimentary and easy to bypass. As a result, the percentage of victims willing to pay the ransom remained fairly low.

Even more tricky, though, was the problem of payment logistics. In ransomware's early days there was no simple, anonymous and

"A TRENDY CRYPTORANSOMWARE SELLS FOR ABOUT $2000 ON DARK NET FORUMS. THIS MEANS THAT AN ATTACKER ONLY NEEDS TO RANSOM EIGHT EVERYDAY USERS (AT THE AVERAGE $300) TO GENERATE A PROFIT."

--The ICIT Ransomware Report [2]

ubiquitous way to receive payment from victims. With fake AV and utilities, crooks could operate under a thin veil of legitimacy, setting up shell corporations to receive credit card payments as semi-legitimate card merchants. Since ransomware was out-and-out fraud, that option wasn't available to receive funds.

However, once the FTC, attorneys general and law enforcement officials started catching up with the scareware ventures around the 2008 timeframe, the cost of business for fake AV and utilities providers started to climb. At that point it made more economic sense for the criminals to opt for the simplicity of ransomware's overt blackmail and begin exploring alternative avenues of payment. That's likely one of the reasons why from about 2010 through 2012 more ransomware scams started cropping up that had victims pay small ransoms through prepaid cash cards, retail shopping cards and even premium SMS texts. These campaigns saw middling success that lead to an increasing but not necessarily explosive growth curve.

Then Bitcoin changed everything.

While it had been under development for several years prior, it wasn't until the end of 2012, when Bitcoin Foundation was formed and Bitcoin Central was recognized as a licensed European bank, that Bitcoin started to hit its stride as a viable form of currency. As it started to gain more mainstream appeal, ransomware criminals recognized it as just the method of monetary extraction they'd been seeking.

Bitcoin exchanges provided them the means of receiving instant payments while maintaining anonymity, all transacted outside the strictures of traditional financial institutions.

The table was set perfectly for the entrance of CryptoLocker in 2013. This revolutionary new breed of ransomware not only harnessed the power of Bitcoin transactions, but combined it with more advanced forms of encryption.

It used 2048-bit RSA key pairs generated from a command-and-control server and delivered to the victim to encrypt their files, making sure victims had no way out unless they paid a tidy sum of about $300 for the key. The Gameover Zeus banking trojan became a delivery mechanism for CryptoLocker. The threat actors behind the botnet were among the first to truly realize the potential value of ransomware with strong encryption, to extend their profits beyond traditional Automated Clearing House (ACH) and wire fraud attacks that target the customers of financial institutions.

CryptoLocker's backers had hit pay dirt, kicking off ransomware's criminal Gold Rush. Cryptolocker Gameover Zeus was shut down in an operation spearheaded by the FBI and technical assistance from CrowdStrike researchers. Even though it was out of operation within seven months of starting, it served as proof to the entire cybercrime community of ransomware's tremendous business upside. This was the true inflection point for ransomware's hockey-stick growth.

CRYPTOLOCKER REVOLUTIONIZED THE RANSOMWARE FIELD BY COMBINING THE POWER OF BITCOIN TRANSACTIONS WITH MORE ADVANCED FORMS OF ENCRYPTION.

The Evolution of Modern Ransomware

2005
First variant of modern ransomware appears in the wild

2006
- Ransomware goes from 56-bit encryption to 660-bit RSA public key encryption

2007

2008
- Scareware dominates with fake AV and rogue utility tools

2009
- Malware evolves from pushing rogue AV to encypting files
- Scam program FileFix Pro extorts $40 to "help" decrypt files

2010
- 10,000 rasomware samples
- Birth of Bitcoin
- Screen-locking ransomware appears

2011

2012
- Over 10,000 ransomware samples
- Ransoms set to $200
- Law enforcement imitation ransomware appears

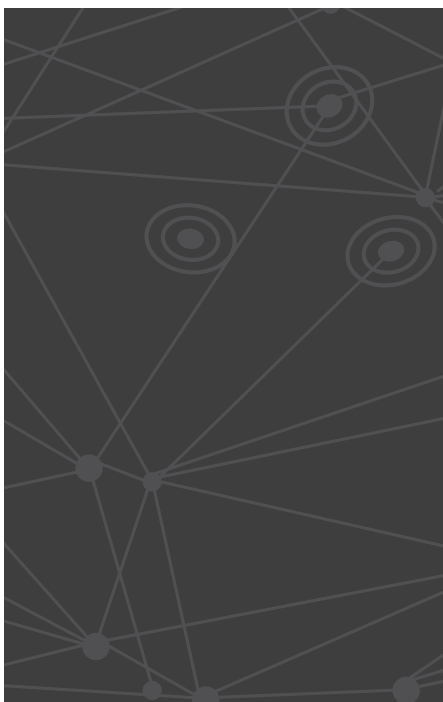
2013
- Over 250,000 ransomware samples
- Cryptolocker appears
- Useage of 2048-bit RSA encryption keys
- Ransomware demands increase to $300
- Crytolocker revenue reaches $300 million in 100 days

2014

2015
- Over 4 million ransomware samples
- Ransomware as a service appears
- Teslacrypt appears

2016
- JavaScript ransomware appears
- Locky rises to prominence
- Hospital pays $17K in ransom
- Ransomware revenue surpasses $1 billion

Within a few months, security researchers were finding copious numbers of CryptoLocker clones in the wild and criminals from all over the world were scrambling to get a piece of the action. Since then, many organized crime gangs have shifted investments and resources from older core businesses, including fake AV, into ransomware operations. The criminal technologists have been working overtime to serve these potential customers by cranking up specialized operations to develop better ransomware code and exploit kit components, flooding Dark Web marketplaces with their wares.



Now that the momentum has built to a critical mass, criminals are going to keep innovating their techniques and expanding their markets. They're getting too rich off ransomware to stop anytime soon.

In fact, they're looking for new ways to tap into even more revenue from ransomware operations, which leads us back to the business risks. Cybercriminals are starting to recognize that if consumers or one-off business users are willing to pay $300 to $500 to unlock run-of-the-mill data on a single endpoint, businesses and other organizations would likely be willing to pay much more for mission-critical data, or to unlock an entire fleet of endpoints held hostage in a single instance.

It's this future risk of ransomware targeting the deeper pockets of businesses that should truly worry enterprise IT leaders.

Where does it go FROM HERE?

With so much money already being made off ransomware by organized crime groups, they've now got a sizeable investment pool ready at their fingertips. They're ploughing these R&D funds into further advancements to help them ensnare even more profitable targets. In fact, these technological advancements have already started to materialize.

As discussed earlier, even the routine ransomware variants found today rely on relatively advanced tactics, techniques and procedures (TTPs) for evading detection and maintaining persistence in the victims' environment as they extract their ransoms. These advanced TTPs include:

- Polymorphism to confound antimalware signature databases with unique hashes and identifiers
- Ample use of "packers" and "crypters" to hide the presence of malicious code
- Anti-monitoring features that can terminate Windows processes like Task Manager, Registry Editor, Command Shell, SysInternals Process Explorer and System Configuration
- Capabilities to check for virtual environments before executing, and executing the malware as child processes to evade sandbox detection
- Use of Tor for command and control communications

These are the typical features found in many variants of ransomware today. But starting early in 2016, ransomware coders have really stepped up their release of innovative and dastardly features. One of the most potent and successful variants to capitalize on these advances is Locky, which:

- Spreads first through malicious Microsoft macros -- and more lately via JavaScript file attachments -- to avoid detection
- Employs RSA and AES encryption, renaming files to unique identifiers in the process
- Encrypts unmapped network drives connected to infected systems
- Deletes all Volume Shadow Snapshots (automatically stored backups), making it impossible to restore files this way
- Obfuscates API calls to hide from static analysis tools
- Hides configuration block storing C&C server static addresses by keeping it obfuscated unless in run-time
- Operates through an affiliate software-as-a-service (SaaS)

Locky is just one vivid example of the lengths to which criminal developers will go to ensure the success of their extortion efforts. Other new variants are introducing their own additional features, as well:

VOLUME SHADOW

is a technology included in Microsoft Windows that allows taking manual or automatic backup copies or "snapshots" of computer files or even complete volumes.

- **Samas:** Leverages vulnerable JBOSS systems to spread across a network and even attack backup files on the network
- **PowerWare:** Encrypts hostage files through "fileless" infection
- **Petya:** Encrypts the Master File Table (MFT) to make the entire system inaccessible
- **Ransom32:** Written in Javascript, making it suitable for cross-platform infection on Mac and Linux
- **KeRanger**: First ransomware targeting OS X, also encrypts Time Machine backup files

Combining Business Savvy with Ruthless Social Engineering

Technology aside, criminals have seized the opportunity to rake in big bucks from ransomware through sophisticated psychological and business tactics. In the past they've won success by playing the roles of successful CEO and evil psychologist at the same time.

Successful Entrepreneur:

On the business front, savvy pricing models have ensured that the ransom amount is as high as possible, without turning away too many potential victims who might give up on their data after a certain threshold. Business tactics now continue to evolve with

the introduction of ransomware-as-a-service affiliate models.

Unethical Psychologist:
On the psychological front, they've preyed on basic human emotions like desperation, fear and even shame to convince users to pay up. Early on, that started out with police-themed scareware that claimed the system was locked by authorities who detected illegal activities using the system. Today the psychological warfare continues to ratchet up. Take, for example, one ransomware scheme that plagued users of the Android Adult Player porn app. It quietly took pictures of users while viewing the app's contents and then displayed that picture on the lock screen along with a ransom demand for $500.

Enterprises should expect this potent cocktail of sharp business acumen and psychological button-pushing to drive more outrageous ransomware schemes during the rest of 2016 and beyond. It's likely what's behind a recent rash of attacks against hospitals and healthcare organizations, which not only are desperate to maintain system uptime from a business perspective, but also for the health and safety of patients, to say nothing of the potential loss of confidence and tarnished brand image that can result from public disclosure of the crime. Ransomware criminals see this as an opportunity to make much more per ransom transaction than from targeting the average user. In one public instance in early 2016 at Hollywood Presbyterian Medical Center, the hospital ended up paying $17,000 to unlock their data[3].

RANSOMWARE PROTECTION MEASURES

CONSIDER OFFLINE STORAGE OF CRITICAL DATA BACKUPS

ROBUST ANTI-PHISHING MEASURES AND EMPLOYEE AWARENESS TRAINING

IMPROVE PATCH MANAGEMENT PROCESSES

It's a powerful proof-of-concept for steeper business ransom demands in the future.

Ransomware's Blight Future

As IT security professionals look to future-proof their businesses for the next ransomware iterations, security pundits warn that they may need to prepare for:

- Cryptoransomware worms that can quickly lock down the contents of an entire network
- Hostage-taking involving highly-targeted and extremely valuable business information for ransom demands of $1 million or more
- Ransomware targeting critical infrastructure utilities
- Ransomware blocking access to major revenue-generating systems such as manufacturing plants or shipping hubs

The online extortion opportunities are only limited by the bounds of the attackers' creativity, and that is proving to be virtually inexhaustible.

What You Need To Know: Protecting Your Enterprise From Ransomware

First of all, it bears repeating that once ransomware encryption has initiated, chances are it's already too late to recover that

MORE RANSOMWARE PROTECTION MEASURES

EMPLOY SOUND ACCESS CONTROLS USING THE RULE OF LEAST PRIVILEGE

RESTRICT WRITE PERMISSIONS ON FILE SERVERS

DISABLE MACROS WHEREVER POSSIBLE IN MICROSOFT WORD

DISABLE PROCESSES LAUNCHING FROM APPDATA AND LOCALAPPDATA DIRECTORIES

data set. Obviously, robust backups are a foundational best practice to prepare for ransomware attacks, but they are no panacea. With variants like Locky, Samas and KeRanger acting as harbingers of future ransomware attacks that can also delete or damage backups, the best medicine for treating ransomware will be preventing an infection in the first place.

Conventional signature-based endpoint protection has already proven itself woefully inadequate at detecting ransomware before it strikes. Additional measures such as whitelisting, Indicators of Compromise (IOCs) or machine learning can each add a nominal degree of improvement over signature-based detection, however they each have their own limitations. For example, in the case of fileless and zero-day ransomware, all of those countermeasures would prove unreliable in detecting or preventing attacks. Furthermore, relying on IOCs, which by definition can only be detected after a compromise has occurred, typically end up alerting IT to the attack after it's too late to make a difference -- in most instances, by the time firm IOCs present themselves, the ransomware has already encrypted its target data.

THE CROWDSTRIKE APPROACH

To combat this escalating level of threat sophistication, **CrowdStrike** uniquely combines multiple methods into a powerful and integrated approach that protects endpoints more effectively against the menace of ransomware. Specifically, CrowdStrike's next-generation endpoint protection solution, Falcon Host, uses an array of complementary prevention and detection methods:

- Blocking known ransomware to weed out common threats with minimum effort
- Exploit blocking to stop the execution and spread of ransomware via unpatched vulnerabilities
- Machine learning for detection of previously unknown, or zero-day ransomware

- Indicators of Attack (IOAs) to identify and block additional unknown ransomware in the early stages of an attack before it can fully execute and inflict damage -- and protect against new categories of ransomware that do not use files to encrypt victim systems

Employing the Power of IOAs

Out of these methods, IOAs are notable because they are fundamentally different from other methods and represent a unique proactive capability. With IOAs, Falcon Host looks for early warning signs that an attack may be underway. Those signs can include code execution, attempts at being stealthy, and lateral movement, to name a few.

IOAs are concerned with the execution of these steps, their sequence and their dependency, recognizing them as indicators that reveal the true intentions and goals of the attacker. IOAs are not focused on the specific tools and malware attackers use to accomplish their objectives since those can change very quickly, as illustrated by the recent surge of ransomware variants.

Furthermore, in the case of fileless ransomware, malicious code is either in a native scripting language or is written straight into memory by legitimate tools such as PowerShell, without being written to disk. This makes it challenging for signature-based methods, sandboxing or even machine learning to analyze. In contrast, IOAs detect the sequences of events that ransomware must undertake in order to complete its mission. This renders moot malware methods such as hiding through leveraging

"known good" system binaries, packing, and binary obfuscation.

In addition, IOAs provide a reliable way to prevent ransomware from deleting backups. This gives users the ability to restore encrypted files, even if file encryption began before the ransomware was stopped.

All this makes IOAs a major breakthrough for ransomware prevention. Instead of trying to fight the futile battle of detecting malware based on the ever-changing contents and characteristics of a ransomware program, IOAs monitor, detect and stop the effects of what ransomware is attempting to achieve before any damage is done. In fact, the IOA approach is so effective and resilient against ransomware iterations that one IOA can cover many variants and versions of multiple ransomware families, including new ones as they are released in the wild.

CrowdStrike's Three Pronged Approach

CrowdStrike employs this combination of protection methods within a layered and integrated three-pronged approach that combines next-generation antivirus with endpoint detection and response (EDR) and managed hunting.

Built-in EDR

Next-gen antivirus provides multiple protections against attacks including ransomware. Simultaneously, EDR acts like a surveillance camera recording what takes place on the endpoint. Any time an endpoint completes an action, whether it is running

an application, connecting to a network, visiting a website or writing a file, Falcon Host's built-in EDR capabilities provide enough data to create a complete picture with the fidelity necessary to find IOAs. The collected activity information is then fed into the CrowdStrike Threat Graph™ data model to analyze and correlate it with billions of events across CrowdStrike's entire customer base, spotting anomalies and detecting IOA patterns to determine if an attack is underway.

Integrated Managed Hunting

This EDR information is used by CrowdStrike's managed hunting team, Falcon Overwatch, an elite organization of experienced security experts who proactively sift through endpoint data to find new hidden attacks that may not immediately trigger automated alerts. It's the holistic nature of these elements working together that provides the ultimate power behind CrowdStrike's capabilities.

Next-Generation Antivirus

CrowdStrike defines next-gen AV as the ability to protect against known and unknown malware, and even attacks that don't use malware. A variety of techniques are combined within next-gen AV: blocking known malware with signatures, blocking unknown malware with machine-learning, exploit blocking and mitigation, and finally, behavioral blocking of malware-free or unknown attacks using IOAs.

ABOUT **CROWDSTRIKE**

CrowdStrike is the leader in next-generation endpoint protection, threat intelligence and response services. CrowdStrike's core technology, the CrowdStrike Falcon™ platform, stops breaches by preventing and responding to all attack types – both malware and malware-free.

CrowdStrike has revolutionized endpoint protection by being the first and only company to unify three crucial elements: next-generation AV, endpoint detection and response (EDR), and a 24/7 managed hunting service — all powered by intelligence and uniquely delivered via the cloud in a single integrated solution.

Falcon uses the patent-pending CrowdStrike Threat Graph™ to analyze and correlate billions of events in real time, providing complete protection and five-second visibility across all endpoints. Many of the world's largest organizations already put their trust in CrowdStrike, including three of the 10 largest global companies by revenue, five of the 10 largest financial institutions, three of the top 10 health care providers, and three of the top 10 energy companies. CrowdStrike Falcon is currently deployed in more than 176 countries.

We Stop Breaches. Learn more: **www.crowdstrike.com**

[1] http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/index.html?section=money_technology

[2] http://icitech.org/wp-content/uploads/2016/03/ICIT-Brief-The-Ransomware-Report2.pdf

[3] http://www.engadget.com/2016/02/19/hospital-ransomware-a-chilling-wake-up-call/

CROWDSTRIKE

crowdstrike.com

15440 Laguna Canyon Road, Suite 250, Irvine, CA 92618

VER. 08.15.16