

DIGITAL BLACKMAIL AS AN EMERGING TACTIC

September 9

2016

Digital Blackmail (DB) represents a severe and growing threat to individuals, small businesses, corporations, and government entities. The rapid increase in the use of DB such as ransomware; the proliferation of variants and growth in their ease of use and acquisition by cybercriminals; weak defenses; and the anonymous nature of the money trail will only increase the scale of future attacks. Private sector, non-governmental organization (NGO), and government cybersecurity experts were brought together by the Office of the Director of National Intelligence and the Department of Homeland Security to determine emerging tactics and countermeasures associated with the threat of DB. In this paper, DB is defined as illicitly acquiring or denying access to sensitive data for the purpose of affecting victims' behaviors. Threats may be made of lost revenue, the release of intellectual property or sensitive personnel/client information, the destruction of critical data, or reputational damage. For clarity, this paper maps DB activities to traditional blackmail behaviors and explores methods and tools, exploits, protection measures, whether to pay or not pay the ransom, and law enforcement (LE) and government points of contact for incident response. The paper also examines the future of the DB threat.

Examining Strategies Public and Private Entities Can Pursue to Contain Such Attacks



2016
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM





Digital Blackmail as an Emerging Tactic

Team Members

Name	Organization
Caitlin Bataillon	FBI
Lynn Choi-Brewer	FBI
James Dean	TrueCourse Advisory Services
Julia Dorosz	WI Department of Justice – Division of Criminal Investigation: Wisconsin Statewide Intelligence Center
Cindy Green-Ortiz	Red Crystal Enterprises
Kurt Jordan	Christian Emergency Network
Eric Kant	Kant Consulting Group
Christopher Porter	FireEye
Aaron Varrone	Cisco



Critical Briefing Paper Findings

“Digital Blackmail is almost a perfect storm of conditions for cyber-criminals – ease of access, use, and distribution of the malware; difficult attribution; high-value targets in low-security environments; and the ease of collection of ransom payments all feed fuel to the criminals as low pressures and warm moist air feed a hurricane.”

Threat Analysis

- Digital Blackmail (DB), in particular *Ransomware*, will be a long-term persistent threat
- The threat horizons have dramatically grown, and continue to grow at a rapid rate
- It is equal opportunity—threatening individuals, nonprofits, corporations of all sizes, government entities, and NGOs
- Threats are non-discriminatory—with a slightly greater focus on sectors with low cybersecurity maturity levels—small/medium-sized firms, NGOs, Healthcare, etc.
- Cybercriminal *Ransomware* kits are economical and easy to access, utilize, customize, and distribute, and virtual currencies make payments non-attributable
- *Ransomware* holds a victim’s high-value targets (data) hostage for low payments
- If not prepared, victims have little choice but to pay or sacrifice the hostage data
- *Ransomware* may be used to maliciously coerce victims by threatening to release sensitive personal information, intellectual property, or information damaging to national security.

“However, the properly prepared individual, company, government, or non-government entity has an excellent chance to detect and defeat an attack or to recover from a successful intrusion. Absent preparation, all is lost.”

Countermeasures Analysis

- The majority of *Ransomware* threats can be mitigated by continuous and strict adherence to standard cybersecurity best practices
- If the threat is successful, recovery is usually possible if proper adherence to backup, recovery, and business continuity best practices have been followed
- There is a growing body of services providing decryption keys for specific malware variants
- Greater outreach is needed by government to all sectors to stress the importance of implementing and adhering to cybersecurity best practices



The Threats We Face

Introduction

Digital blackmail (DB) is illicitly acquiring or denying access to sensitive data for the purpose of affecting or controlling a person's, company's, or government's behavior. Blackmail can threaten lost revenue, the bulk release of sensitive data, or leaked embarrassing information, prevented only by a financial payoff to the attackers. DB may originate from insider threats, individual hackers, organized cybercriminal organizations, hacktivists, and state-sponsored actors. The tools for executing a ransomware attack are not only easy for an attacker to obtain and use, but are also relatively inexpensive.

Although "*ransomware*" for criminal financial gain naturally first comes to mind when we think of DB, there are many other types of DB that may play out.

- Attackers threaten to publicly release incriminating images or communications (e.g., "sextortion," an already prevalent crime in Asia and Europe) unless a government official provides sensitive information (such as passwords to classified systems). Incriminating data could be personal, or that of close friends or relatives who have had their systems compromised by intrusive malware.
- A military service member who receives an electronic threat that hostages will be killed or an attack will be carried out if sensitive military data is not revealed.
- A government official receives a malware threat that attempts to coerce a change in Government policy/activity or sensitive/damaging information about the Government will be publicly released.
- A high-volume program trader is threatened by malware to execute high-volume trades that can affect market activity—as in the "flash crash"—and destabilize the financial system or produce illegal gains for criminal cartels or terrorist organizations.
- A broker who has access to hundreds of high-value funds is coerced by malware to transfer funds to a terrorist organization.
- The 2014 North Korean extortion cyber attack against Sony Pictures Entertainment threatened the company with brand destruction.



- An executive of a major financial services firm (or hospital, as has been prevalent recently) is subjected to DB, threatened with the release of sensitive personal information about specific, high-value customers in furtherance of state-sponsored or hacktivist agendas.

Obviously, traditional blackmail is one of the oldest forms of coercion. Much is known about that threat, which can be applied to today's electronic version. However, DB differs from traditional blackmail in its ease of development and delivery, the speed and volume of attacks that can be mounted simultaneously, and its unique detection challenges. Still, DB has much commonality with traditional blackmail in the techniques used to extort (i.e., money, ideology, compromise, ego) and its goals (intelligence gathering, destabilization of the social fabric, influencing behavioral or policy change, financial gain, etc.). As such, it is useful to keep in mind that, although the medium of delivery is different, DB is still a traditional crime.

Although this briefing paper focuses on financially-driven ransomware, executives of businesses and government institutions should keep in mind the other types of DB to which they may be subjected. Fortunately, the majority of the mitigation approaches outlined in this paper are effective against non-financial blackmail as well as financially-oriented blackmail.

Despite the fact that ransomware is increasing at a dramatic rate, the mitigation approaches outlined in this paper, such as maintaining common cyber-hygiene techniques, utilizing good backup procedures, conducting anti-phishing training, and formulating a comprehensive Business Continuity Plan, are all standard cyber best practices—nothing new or extraordinary. If applied with good management discipline, these best practices can be very effective against many cyber threats.

Ransomware – Types and History

Ransomware has developed significantly since the first observed ransomware incidents in 1989, from simple blockers targeting Russian-speaking individuals to sophisticated encrypting ransomware types affecting individuals and businesses globally. The evolution of ransomware has been greatly influenced by ever-changing developments in culture, economics, security, and technology over time.

In the past, malware was never specifically focused on the destruction of, or denial of access to, data held in the systems it infected. Most actors were primarily concerned with getting continued access to the data or the resources a system provided. Ransomware, however, has shifted this focus toward extortion. Actors are now denying access to data and demanding money in order to restore users' access to this data.¹



Definition

Ransomware is a class of malware that has an end-goal of denying access to user data by specifically targeting user files but avoiding damage to system files. Ransomware behaves this way for two reasons: to ensure the user can be contacted and notified of what happened to her files, and to provide a way for the user to pay the ransom to regain access to her files.¹

There are two basic types of ransomware in circulation. The most common type today is crypto ransomware, which aims to encrypt personal or corporate data and files. The other type, known as locker ransomware, is designed to lock the computer, disable a program or function on the device, and prevent victims from freely using the device.³

Crypto Ransomware

This type of ransomware is designed to find and encrypt valuable data stored on the computer, making the data useless unless the user obtains the decryption key. As digital technology increases, more and more important data is stored on personal and business computers and devices. Many users are not aware of the need to, or know how to, create backups to guard against theft or loss of the computer or hard disk failures. Even a smaller number of users are aware of the need to protect against a possible crypto ransomware attack. Many companies are unaware of how vulnerable their networks are until it is too late, and they have already become a victim.³

Crypto ransomware targets these weaknesses in the typical user's security posture for extortion purposes. Creators of crypto ransomware know that data stored on personal or business computers is likely to be important to individual users or the company overall. Ransomware victims may be desperate to get their data back, preferring to pay the ransom to restore access rather than simply lose it forever and suffer the consequences. For some businesses and other agencies who do not have strong cybersecurity—for example, a company that deals with personal information in order to provide services but has no backup of client lists, a healthcare provider that cannot access patients records, or a law enforcement agency that cannot access case files—paying the ransom may be the only option to recover lost data.³

After installation, a typical crypto ransomware threat quietly searches for and encrypts files. Its goal is to stay below the radar until it can find and encrypt all of the files that could be of value to the user. By the time the victim is presented with the malware's message that their data is encrypted, the damage is already done.³



With most crypto ransomware infections, the affected computer continues to work normally, as the malware does not target critical system files or disrupt the computer's functionality. Users can still use the computer to perform a range of activities apart from accessing the data that has been encrypted.³

Locker Ransomware

Locker ransomware is designed to deny access to computing resources, usually by locking the user interface of the computer or device, then asking the user to pay a fee in order to restore access. Locked computers will often have limited capabilities, such as only allowing the user to interact with the ransomware and pay the ransom.³

Locker ransomware is typically only designed to prevent access to the computer interface, largely leaving the underlying system and files untouched. Therefore, the malware could potentially be removed to restore a computer to something nearing its original state. In this way, locker ransomware is less effective at extracting ransom payments compared to its more destructive relative crypto ransomware.³

Because locker ransomware can usually be removed cleanly, it tends to go to great lengths to incorporate social engineering techniques that pressure victims into paying. This type of ransomware often masquerades as law enforcement authorities and claims to issue fines to users for alleged online indiscretions or criminal activities.³

ORIGIN

Despite only receiving significant media attention in the past few years, ransomware has existed for at least 26 years. The first publicly reported ransomware sample was observed in 1989, when a medical doctor wrote and shared a type of encrypting ransomware via a floppy disk, called the AIDS Trojan. However, ransomware remained scarce until around 2005, when reports surfaced about attacks against Russian-speaking individuals. It is unclear exactly how ransomware spread at this time, but owing to the language limitation, reports indicated that targeting did not extend beyond Russian speakers.²

The first instances of misleading applications began to appear in 2005, posing as fake spyware removal tools (e.g., SpySheriff) or performance enhancement tools. These applications typically exaggerated the impact of computer issues and said they would resolve them if the user paid for a license, usually between \$30 and \$90. In reality, either there was no issue or the software was not actually functional.³



2016 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

In early 2005, the first set of modern crypto ransomware appeared, using a symmetric encryption algorithm. In other words, the same key was used for both encryption and decryption, making it easy to overcome. By early 2006, crypto ransomware was already evolving into variants like Trojan.Cryzip, which would copy data files to individual password-protected files and delete the originals. However, at the time, the password was written into the Trojan itself, making it also easy to overcome.³

Ransomware began gaining widespread attention in 2008 and 2009 with the release of fake antivirus programs that mimicked the appearance and functionality of legitimate security software. These programs would perform fake scans and find large numbers of threats to the computer systems, then ask for payment between \$40 and \$100 to fix the fake problems.³

Reports of ransomware in other countries have grown significantly since 2009. By 2012, ransomware frequently targeted highly developed countries, most likely owing to three factors. First, the introduction of ransomware builders allowed more individuals to create their own variants. Second, the success of GPCode and other ransomware attracted other cybercriminals to ransomware schemes. Third, the ransomware marketplace developed to the point where ransomware developers rented out their malware to other cybercriminals and used botnet-based distribution tactics (e.g., spam or secondary payload installation) to infect significantly more targets.²

In 2011 and 2012, cybercriminals moved away from antivirus tools and toward locker ransomware. They disabled access and control of the computer and requested payment of around \$150 to \$200 to unlock the device.³

From 2013 to the present day, there has been a shift back to crypto ransomware. The threats usually display an extortion message, offering to return data upon payment of around \$300 for a single computer. These variants are much more capable than earlier versions, with stronger operational and encryption procedures.³

Current ransomware operations target geographic regions all around the world. In recent months, ransomware campaigns have targeted many countries, including Japan, Korea, Malaysia, Russia, the United Kingdom, Australia, Brazil and the United States.

Ransomware operations are also beginning to impact previously untargeted countries. In particular, ransomware is increasingly targeting East Asian nations. Major ransomware families typically expand their operations over time, shifting from country to country to both broaden their target pool and provide some defense against law enforcement activities in particular countries.²



2016
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

In 2015, the top six countries impacted by all types of ransomware were the United States, Japan, the United Kingdom, Italy, Germany, and Russia.³

As devastating as it may be to an individual user to lose all of his personal files, larger companies and government agencies are equally at risk. Cybercriminals may need just *one* employee to accidentally click a malicious link in a phishing e-mail in order to gain access to an entire network. While prevention and mitigation measures are discussed later in this briefing paper, it bears mentioning here that, in today's world of DB, it is absolutely crucial to retain backups of data in off-site locations or cloud-based storage systems to ensure data is not vulnerable to a single user error.



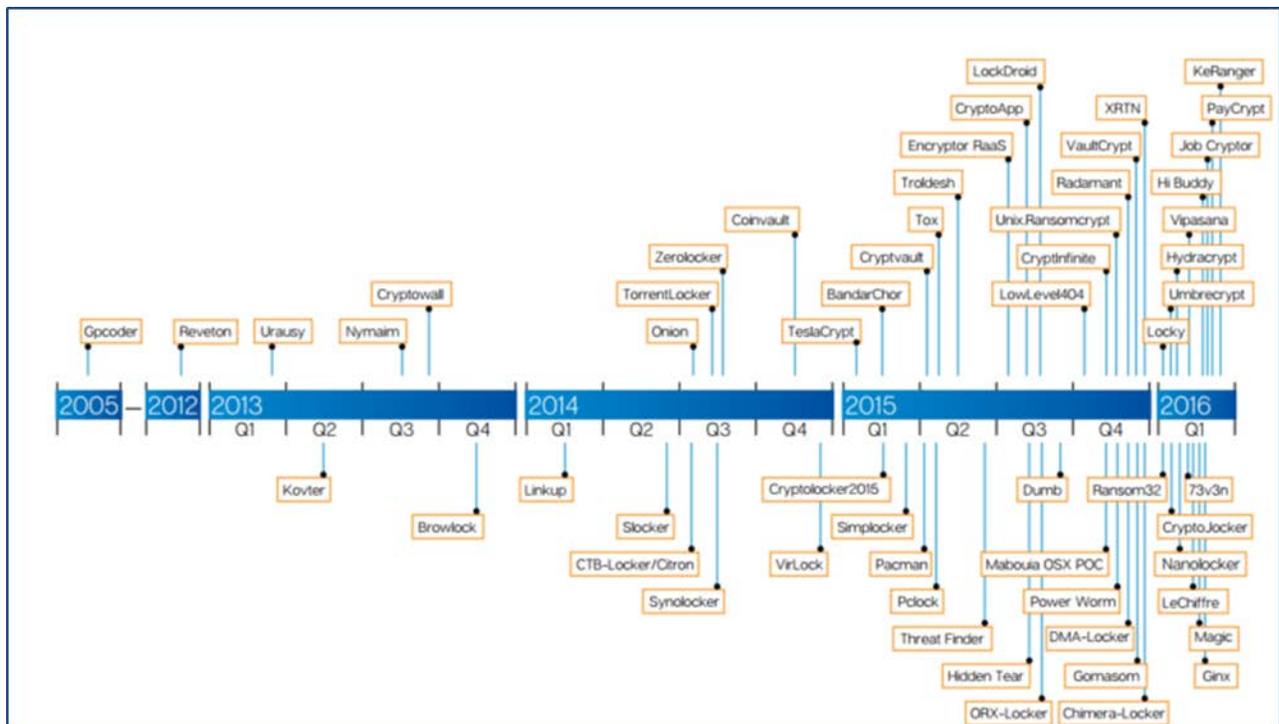


2016 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

Evolution of Ransomware

The following chart depicts the aggressive increase of ransomware tools available to cybercriminals.

There is no anticipated reduction in the rate of new tools that will become available through the dark web.



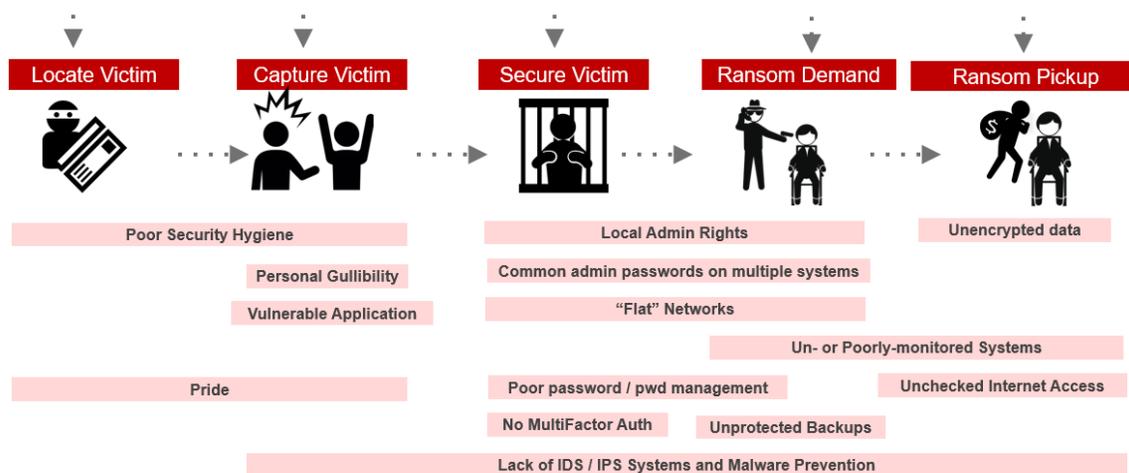
Source: Chris Olive. (2016). [The \(Immediate\) Future of Ransomware.](#)



THE ATTACK

The way malicious actors spread ransomware depends on the device affected by the malware and the resources available to the actors. Ransomware campaigns continue to primarily target Windows and Android devices. The current variants of ransomware seen today tend to attempt to infect as many victims as possible rather than purposely targeting specific sectors or businesses.² Opportunistic or targeted, the results of ransomware to the victim are the same.

Ransomware: Methods and Tools

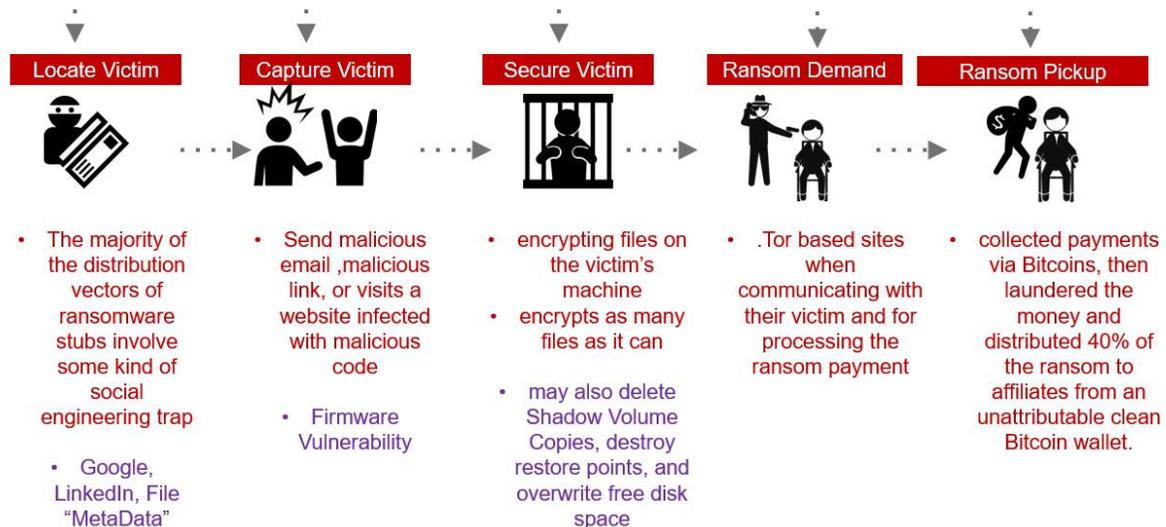


Ransomware can be delivered through exploit kits, watering hole attacks, malvertising, or mass phishing campaigns. Once delivered, ransomware typically identifies user files and data via a sort of embedded file extension list. However, it specifically avoids certain system directories to ensure system stability so that the victim may complete payment of the ransom.¹

Once the malware has encrypted the files, it usually self-deletes, leaving behind a document that instructs the victim on where and how to provide payment to get her files back. Some variants show their victim a countdown timer, with threats to increase the ransom or to delete the decryption key if payment is not received in time.¹



Ransomware: Exploits Used



Multiple actors are also using social engineering techniques, such as spoofing updates to various web browsers and applications, to "trick" users into installing the ransomware.²

Ransomware affecting mobile devices typically spreads by socially engineering victims into downloading fake applications, especially those with adult themes or are associated with adult-themed websites. Social engineering tactics include masquerading as law enforcement operations or spoofing legitimate application updates that require the victim to enter confidential information. Mobile ransomware is also distributed via SMS messages, spam e-mails, and within other forms of malware, such as credential theft software. Because Android and iOS mobile operating systems require approval by the device's owner to download an application and allow certain permissions on the device (absent use of an exploit), the growth of mobile ransomware distribution will almost certainly be determined by the development of social engineering campaigns. A variety of mobile ransomware variants employ blocker techniques. One example of a type of Android malware that spoofs legitimate application updates is the GM Bot. This botnet includes a ransomware capability in which the victim is told that he must provide credit card information to update Google Play, and the malware blocks normal use of the phone until the data is provided.²



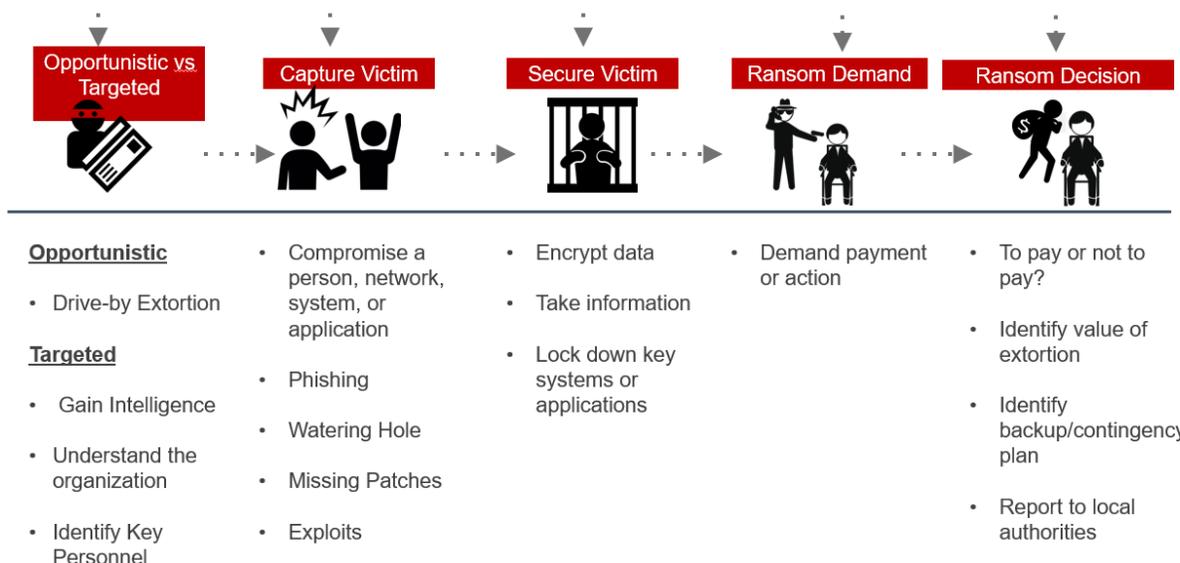
PAYMENT METHODS

The use of direct and anonymous electronic payment methods has been a key factor in making ransomware a profitable cybercrime activity. Ransomware developers have previously used a range of payment systems including Qiwi, WebMoney, PerfectMoney, Ukash, PaySafeCard, MoneyPak, CashU and Reloadit.²

In 2014 and 2015, Bitcoin became the preferred payment method for many ransomware developers, to the exclusion of other payment methods. Many criminal actors prefer to use Bitcoins for a variety of illicit activities because they are difficult to trace and help to obfuscate the malicious activity.²

Another recently observed development in ransomware payment schemes involves a fluctuating ransom price. Historically, once ransomware has infected a machine, it requests the full amount up front in order for users to gain access to their locked files. However, there has been some deviation from this trend. For example, one recently observed type of ransomware includes a price increase every day until the ransom is paid. Other ransomware samples reportedly change their ransom price after victims fail to pay by a deadline. Also observed are ransomware kit authors claiming they will raise the ransom price based on the number of attempts the victim makes to recover the stolen data, though this approach could be difficult and such price hikes have not been confirmed.²

Digital Blackmail: Activities





First Lines of Defense

In the movie *Spy Game*, Robert Redford’s character asked the rhetorical question, “*When did Noah build the Ark?*”—to which he replied, “*Before the flood, before the flood!*” There are few better adages for a ransomware attack. If not prepared for an attack, there will be few options to the victim except to sacrifice the files or pay the ransom.

However, for properly prepared firms, the majority of attacks can be detected and deterred, and even if they are not defeated, recovery is very likely. There are a number of steps to implement, but almost all of them are standard cyber-hygiene and IT best practices. In addition, these protections are effective against many cyber threats and all forms of DB, not just ransomware. From a cost effectiveness perspective, implementing these actions has excellent economies of scale.

There may seem to be a lot of tasks to conduct and put in place. However, DB will be a threat for a long time to come. To put the threat in context, extortion attempts have been documented since the 12th Century, and we are still combating them today. Therefore, it is recommended that an organization conduct gap analysis between its current preparations and those outlined in this or other publications. The organization should then develop a 12- to 18-month (or longer) duration plan with quarterly goals to bridge the gaps. This plan will be unique to each entity depending on its current capabilities, staffing, budget, risk acceptance levels, threat assessments, etc.

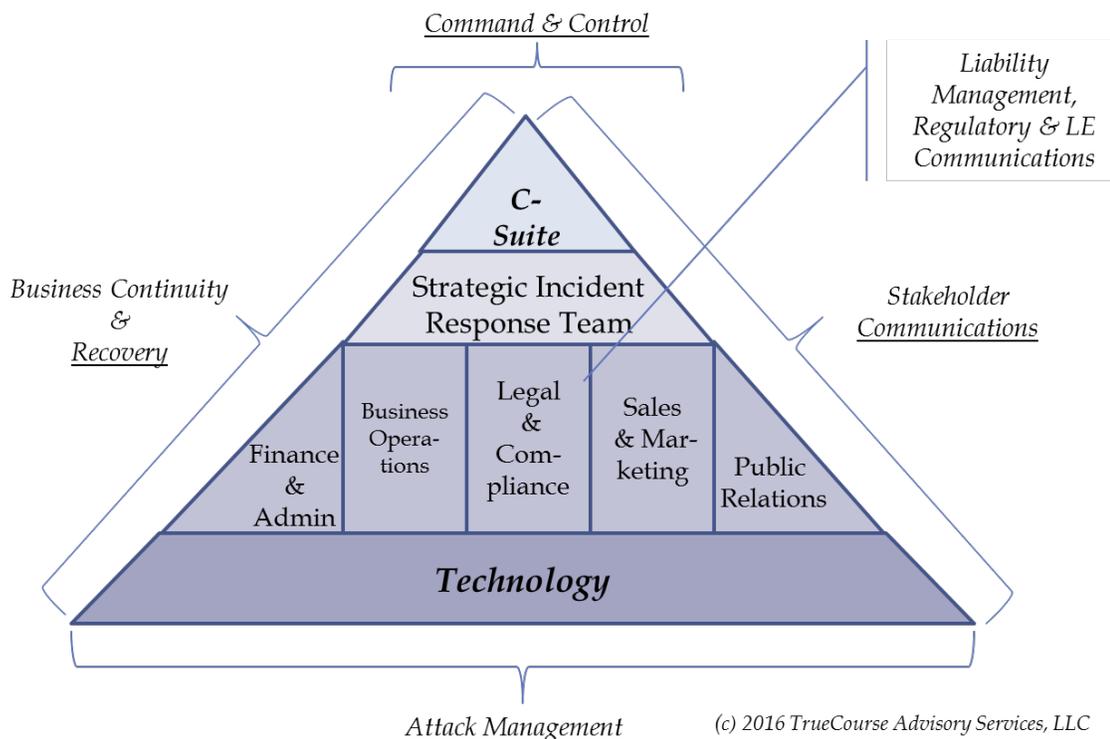




Prevention Management

Often overlooked are several practices that must be in place or authorized by senior management prior to an event occurring, be it general cyber attack or DB. First and most important is an understanding that, although a cyber attack is a technology event, it is an attack against the corporation and its assets, and the response needs to be driven by business management, not just the technology team. The following items address the management activities related to cyber attack prevention management.

1. Establish a Policy and Incident Response Team – If not already in place, create an executive team that will define policies and provide direction and decision-making in the event of an incident. A sample structure for such a team is shown below.



Each firm's structure will be unique, but as depicted, an attack may involve all aspects of the business. Establishing the relationships and protocols before an incident is essential to a quick and effective recovery.

2. Intelligence Gathering – Threats, sources, and methods are constantly changing in the world of ransomware, so gathering intelligence and developing a threat



2016 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

matrix and various attack scenarios for the firm are an important first step in developing a preventive strategy. Joining industry and government associations is a good source of relevant industry intelligence. Examples include FBI InfraGard, the appropriate Information Sharing and Analysis Center (ISAC), the National Cyber-Forensics & Training Alliance (NCFTA), and many other available organizations. Of course, latest intelligence is also available from the commercial cybersecurity sector.

3. Develop a Prevention and Preparation Strategy – Developing and publishing an overall strategy for attack prevention and preparation will ensure an integrated and cohesive approach to managing and responding to a threat. It will ensure each group within the firm knows its role and responsibility and help mitigate mistakes made in the heat of an attack.

First creating an inventory of mission-critical files and systems will help prioritize other aspects of the strategy. Another important part of the strategy is to define which security standards (NIST, ISO2700x, PCI-DSS, etc.) the firm should maintain, both internally and for third parties, and to ensure they meet any insurance requirements for future cyber attack insurance claims.

Further, a policy for decision-making regarding the payment of a ransom should also be developed early on. Financial impact, the culture of the company, branding, and law enforcement concerns should also be a key part of the payment strategy. The strategy should also include a methodology for ranking the degree of risk posed by an incident. Is the incident isolated to one computer or the entire network and backups? Does it affect third parties? The threat ranking will help determine the level of response needed.

4. Establish an Incident Response Plan – This step should consist of a series of protocols (or “playbooks”) based on the level of threat the attack poses, from single desktop infection to an enterprise-level encryption attack. If a scenario requires attribution, it is critical to bring in a professional cyber-forensics consultant early, as significant evidence may be lost through an ad hoc stabilization or recovery process.
5. Establish an Incident Communications Network – It is of significant benefit to a victim company to have a pre-positioned network of trusted individuals that can be contacted for expertise and advice related to an attack. These can include cybersecurity consultants, public affairs and media consultants, legal firms specializing in cybersecurity, law enforcement, and regulatory officers.





2016 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

Establishing relationships before they are needed and having a network that is familiar with the response operations can be invaluable during a challenging event.

6. **Conduct Business Continuity Planning** – This step is often confused with backups and recovery, but it is entirely different. Business continuity planning addresses how the business will continue to run if systems are not available and the recovery time is significant. Identifying critical business operations and developing workarounds and alternative methods of documenting critical transactions are all part of a good business continuity plan. Client and third-party communications are also important. Conducting desk-top (a.k.a., tabletop) scenarios will help validate the plan and itemize deficiencies.
7. **End-User Training** – The majority of ransomware is delivered as a result of poor user cyber-hygiene. Responding to phishing e-mails, clicking links embedded in e-mails, non-secure browsing activities, and keeping critical data on local drives that are not corporately backed up are all common sources of compromise. Regular training, awareness campaigns, and Employee Behavioral Penetration Testing are effective prevention tools.
8. **Communication Planning** – Although ransomware attacks are often thought of as internal events, depending on the scale of the attack and taking into consideration the full scale of DB, an incident could affect relations with third-party vendors, clients, the general public, shareholders, service providers, and others. In a pre-planning exercise, developing a number of different attack scenarios and determining which entities will need to be contacted is important. Identify who within the third party to contact, who within the firm is responsible for making contact, and what form of media (phone, e-mail, public notice) should be used. Determining the legal implications of the communications and content beforehand can spare the company from unnecessary liability and expense arising from a future event. As part of the pre-planning effort, identifying which law enforcement agency to contact and developing a relationship with a point of contact can be very valuable when and if an event occurs.
9. **Legal and Insurance Planning** – It is also best-practice to have the legal team review the scenarios and provide guidance as to potential liability issues, communication protocols, documentation of incident actions, and approvals. It is also critical to ensure legal departments review and approve threat information and other actionable intelligence strategies shared with peer groups, peers, and law enforcement. Depending on the insurance coverage a firm may have, ransom payments, lost income from business interruption, costs related to recovery, and even the ransom itself may be recoverable if certain actions and communications





are taken during the event. To maximize insurance claim recovery, this information should be contained in the response scenarios so that proper communication and documentation are maintained during an event.

Prevention Activities

There is a large body of work available on best operational practices related to ransomware. These best practices will constantly change, and at a rapid rate, owing to the accelerated changes in threats and the technology environment. However, the following are core best practices that should be applied at an operational level.

1. Backups/Contingency Planning – A backup policy/contingency plan, procedure, and technology for systems should be developed and utilized in the event data loss occurs. Unfortunately, many companies do not effectively test their recovery plans, which should be done on a regular basis. Other key points include ensuring backups are kept offline; plans are made for mobile, local, server and cloud-based files; and backups are made on a regular basis, considering the application requirements.
2. Patching Life Cycle – A patching level cycle should be utilized to deploy updates to all systems for known Common Vulnerabilities and Exposures (CVE) in commonly used software such as, but not limited to: Adobe Flash, Adobe Acrobat, Microsoft Silverlight, Oracle Java, Microsoft Internet Explorer, and Microsoft Office; where exploits can take advantage of programmatic errors and unsecure code.
3. Remediation/Upgrade Plan for Unsupported Operating Systems (OS) – Develop a remediation/upgrade plan for unsupported and unpatched OS such as Windows XP, Windows 2000, and Windows 2003, or consider the use of application whitelisting.
4. Proactive Host-Based and Network-Based Security Defenses – Each system should be protected with an updated Anti-Virus Scan Engine, Virus Definitions/Signatures, and a Host-Based Firewall solution for detecting and preventing the latest ransomware variants. Behavior-based antivirus solutions may also be examined. At an organizational level, a Network Intrusion Detection/Prevention System (IDS/IPS) and a Network-based Firewall should also be utilized to detect and prevent the latest ransomware variants. Based on victim interviews, the addition of SSL scanning to the Network-based Firewall has stopped additional ransomware attacks.



2016
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

5. DNS (Domain Name System) Service Protection – Consider configuring the use of a Public DNS service on systems, such as Google Public DNS or OpenDNS, that provides phishing protection and content filtering of unknown domains. The service is an additional layer of security to assist with preventing attacks by expanding threat protection beyond the perimeter.
6. Network Segmentation – Segmenting the network will help limit an attack from spreading through the entire enterprise or to third parties with network connections.
7. Disable macros – Disable all macro scripts from files sent via e-mail. Implement software restriction policies or other controls to prevent programs from executing from common ransomware locations.
8. Limiting Internet Access – Restrict access to the Internet to only those systems with a need for access.
9. Limit Administrator Rights – Only provide administrator rights as needed based on the principle of least privilege.



Attack Response

Depending on how well an organization or individual is prepared, the response to an attack can range from panic, confusion, and chaos to a calm, methodical approach to recovery. The following are key steps when confronted by an attack.

1. Immediately Isolate the Infected Device – Remove it from the network to prevent propagation of the infection to the network and shared drives.
2. Immediately Secure Backup Data – Take backups offline or remove them from the system (if they are connected to the network).
3. Activate Incident Response Team – Notify the team of the attack status and initiate the incident response plan.
4. Assess and Classify the Threat – The level of response and the number of individuals and third parties affected will vary according to the level of the threat. A single infected desktop computer with a low-value ransom will have a much lower response activity than a network-level infection or backup encryption at a corporate level.
5. Determine if the Threat is Isolated – Adversaries may use multiple attack vectors to distract the victim from the true attack, which could range from exfiltration of valuable intellectual property or illicit wire transfers to overseas accounts. While evaluating the threat, do not fall prey to tunnel vision; take actions to determine if any other unusual activities or incursions are occurring.
6. Collect details on specifics of the infection, including:
 - a. the ransomware variant
 - b. when the infection occurred
 - c. how you believe the infection occurred (i.e., infection vector)
 - d. what data was encrypted
 - e. which scenario matches the attack pattern
 - f. indicators that may help identify the attackers (e.g., Bitcoin wallets, URLs used to communicate with the attackers, suspicious IP addresses)
7. Research Variant Type – Determine if decryption keys or processes are available for the responsible malware variant. There are several services and websites (such as nomoreransom.org) that provide access to keys and solutions to encrypted data.



2016 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

8. Determine Course of Action – Based on the information obtained in items 5-7, select the appropriate protocol or playbook to activate.
9. Execute Notifications – Depending on the protocol selected, one of the first steps will be notifying appropriate external parties, potentially including cyber-forensic consultants, the incident communication network, law enforcement, intelligence-sharing organizations, insurance companies, and external law firms. One team member should be assigned to manage or coordinate these communications to ensure a consistent message and coordinated assessment of responses.

NO MORE RANSOM!

NEED HELP unlocking your digital
life without paying your
attackers*?

YES

NO

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!

Recovery Services

There are several services and websites (such as nomoreransom.org above) that provide access to keys and solutions to encrypted data.



Involving the Federal Government

The FBI encourages organizations to contact a local FBI field office immediately to report a ransomware event and request assistance. The FBI has a Cyber Task Force (CTF) in each of the 56 field offices across the country that can deploy agents, analysts, and computer scientists to address cyber incidents. Victims are also encouraged to report cyber incidents to the FBI's Internet Crime Complain Center (IC3), which supports a mechanism for the public to submit information to the FBI concerning suspected Internet-facilitated criminal activity. Reporting even unsuccessful or past ransomware incidents could help the FBI to identify, pursue, and ultimately defeat the actors responsible. As part of an incident response plan, organizations should consider under what circumstances to involve the Federal Government and ensure concurrence from appropriate members of the incident response team, especially legal, information security, and privacy representatives.⁵

In July 2016, the Obama Administration released Presidential Policy Directive 41 (PPD-41), which established a unified federal government response to potential cyber incidents. When responding to a cyber incident, federal agencies are responsible for three concurrent services: threat response, asset response, and intelligence support and related activities. The first two services are especially relevant to victims when considering Federal Government assistance during a cyber incident.⁶

- The Department of Justice, through the FBI and the National Cyber Investigative Joint Task Force (NCIJTF), is the designated lead for threat response activities, which include the investigative action related to cyber incidents, such as collecting evidence, determining attribution, conducting law enforcement activity, and identifying opportunities for further investigative action, intelligence gathering, and threat pursuit and disruption.⁶
- The Department of Homeland Security, through the National Cybersecurity and Communications Integration Center (NCCIC), is the designated lead for asset response activities, which include mitigation of vulnerabilities and identification of potential risks to other organizations or sectors that may be affected.⁶
- PPD-41 acknowledges threat and asset responders will share some responsibilities and activities. Furthermore, victims in need of assistance should trust that the Federal Government coordinates to ensure no single point of failure in response. As such, whichever agency first becomes aware of a cyber incident is required to rapidly notify other relevant agencies to ensure the optimal level of response.⁶



2016 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

Importantly, two of PPD-41's guiding principles for cyber incident response are to respect and limit disruption to victims. In other words, to the extent permitted by law, Federal Government responders will safeguard details of the incident and sensitive private sector information, as well as generally defer to victims in notifying other affected private sector entities and the public. Furthermore, federal response activities will balance investigative and national security requirements, public health and safety, and the victim's need to return to normal operations as quickly as possible.⁶

Victims in need of threat response can prepare for their interaction with the FBI. You should establish a trusted partnership with the local FBI field office prior to a cyber incident. Such a partnership will not only allow you to receive FBI warnings about targeting activity and technical indicators to help defend your network, but it will ensure you have a trusted contact in the FBI who is responsive to and understands your needs in the event of a cyber incident. It is also important to maintain sufficient logging on your network to facilitate the FBI's investigation. Tailor your logging toward your own organization, and try to preserve and/or heavily monitor ongoing malicious activity. Your FBI contact can ensure you understand what logging is needed. Finally, it is very beneficial to the FBI to have appropriate company personnel—including network security personnel, computer incident response teams, network administrators, and corporate law teams—ready to assist in order to speed along the FBI's investigation.⁷

With regard to state, local, tribal, and territorial (SLTT) government response, SLTT law enforcement usually will refer cyber incidents to the FBI because many cyber incidents involve attackers outside SLTT jurisdiction, larger schemes impacting victims in other jurisdictions, and federal statute violations. Per PPD-41, SLTT governments have responsibilities, authorities, capabilities, and resources that can be leveraged in response to a cyber incident, so the Federal Government should be prepared to partner with SLTT governments when responding to an incident.⁶





Key Federal Points of Contact:

Threat Response	Asset Response
<p>Federal Bureau of Investigation (FBI)</p> <p>FBI Field Office Cyber Task Forces: http://www.fbi.gov/contact-us/field</p> <p>Internet Crime Complaint Center (IC3): http://www.ic3.gov</p> <p><i>Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to the FBI Field Office Cyber Task Forces.</i></p> <p><i>Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.</i></p>	<p>National Cybersecurity and Communications Integration Center (NCCIC)</p> <p>NCCIC: (888) 282-0870 or NCCIC@hq.dhs.gov</p> <p>United States Computer Emergency Readiness Team (US-CERT): http://www.us-cert.gov</p> <p><i>Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.</i></p>
<p>National Cyber Investigative Joint Task Force (NCIJTF)</p> <p>NCIJTF CyWatch 24/7 Command Center: (855) 292-3937 or cywatch@ic.fbi.gov</p> <p><i>Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government.</i></p>	





When Does it Pay to Pay?

There is obvious controversy in the debate over whether or not to pay a ransom. The better a company's prevention strategies, the better the chance they will not face this dilemma.

FBI Comment

"We do not encourage paying a ransom. We understand that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers."⁹



Some reasons listed in the brochure as to why the FBI discourages the ransom payment include:

- *"Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom.*
- *Some victims who paid the demand have reported being targeted again by cyber actors.*
- *After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key.*
- *Paying could inadvertently encourage this criminal business model."*⁹

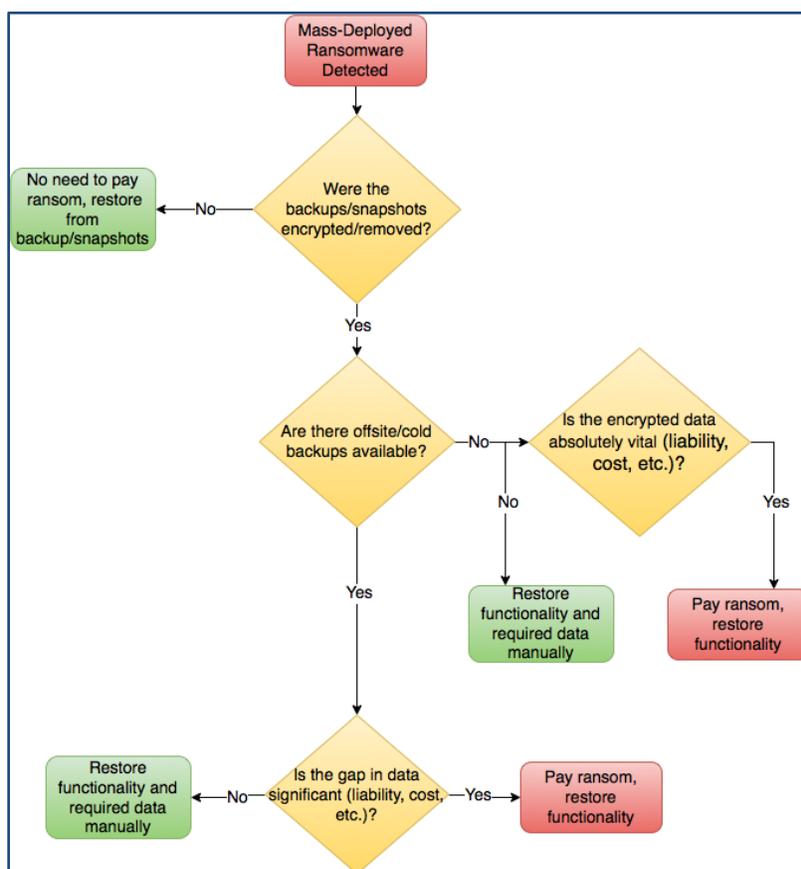
It is important for each firm to develop its own policy for ransom payment based on threat level as a part of their threat assessment and prevention strategy efforts. Each company will have to evaluate their need to pay a ransom based on several factors unique to the organization and the threat, including:



2016 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

- Culture of the company related to criminal activities
- Condition of backup/recovery capabilities
- Value of affected data
- Reputational damage from publication of the incident
- Recovery time implications
- Third-party impacts
- Price of the ransom
- Reputation of the ransom attacker

One decision table to assist companies making a decision related to payment is shown below.



Source: Cisco Talos



Rule of Thumb

“If the cost associated with paying the ransom is less than the cost associated with the loss of data for that gap of time between off-site backups, then in all likelihood, the organization will pay the ransom. Otherwise, the organization will accept the loss and begin the recovery process.” (Source: Cisco Talos.)

If a firm elects to pay a ransom, then prior to the payment, and depending on the amount of the payment, the company’s insurance carrier should be contacted. The actual cost of the ransom may be covered under business interruption or other clauses, but usually only if the insurance approves the payment before it is made.

Conclusion and Future Considerations

DB will be a serious threat for some time to come. It is almost a perfect storm of conditions for the criminals; ease of access to the code, ease of use and distribution, difficult attribution, high-value targets in low-security environments, and the ease of ransom payment collection all feed fuel to the criminals as low pressures and warm moist air feed a hurricane.

In addition to the status quo, the attacks may get darker and deeper. New vectors may attack everything connected to a network, including backups and cloud storage, increasing the value of targets to adversaries. Alternative encryption methods are also being explored by attackers, including master boot record and metadata encryption.



On the positive side, the Boy Scouts have the answer: “*Always Be Prepared!*” ***The properly prepared individual, company, or government entity has an excellent chance to detect and defeat an attack, or to recover from a successful intrusion.*** The majority of the preparation activities are standard IT best practices that are well-known, documented, and tested. It is critical that individuals, companies, and government entities, to protect themselves from this growing and ever menacing threat, exercise strong discipline in consistently applying the cybersecurity best practices covered in this briefing paper to their cyber environment.



References

1. Digital Blackmail as an Emerging Tactic Team Slides.
2. Cisco Talos. (11 April 2016). *Ransomware: Past, Present, and Future*.
3. FireEye, Inc. (27 July 2015). *Overview of Ransomware History and Current Trends*.
4. Symantec. (6 August 2015). *The Evolution of Ransomware*.
5. Department of Justice, FBI. (4 May 2016). *Ransomware*.
https://pdf.ic3.gov/Ransomware_Trifold_e-version.pdf.
6. The White House, Office of the Press Secretary. (26 July 2016). *Presidential Policy Directive – United States Cyber Incident Coordination*. <https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>.
7. FBI, Cyber Division. *Incident Preparedness: Building alliances to improve the nation's cybersecurity*. Handout.
8. Department of Justice, FBI, IC3, NCIJTF, Department of Homeland Security, USSS, Homeland Security Investigations, NCCIC. (11 August 2016). *Cyber Incident Reporting, A Unified Message for Reporting to the Federal Government*.
<https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf>.
9. FBI. (29 April 2016). *Ransomware: What It Is and What To Do About It*.
<https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise>.



2016 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

Further Reading

- FBI, <https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise>
- ODNI, Intelligence Community Analyst – 2014 PPS – “Understanding Cyber Threats”
- NJCCIC, <http://www.cyber.nj.gov/threat-analysis/ransomware-an-enduring-risk-to-organizations-and-individuals>
- NJCCIC, <http://www.cyber.nj.gov/threat-analysis/ransomware-lucrative-cyber-crime-tactics-rapidly-evolving>
- Sophos, <https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-current-state-of-ransomware.pdf?la=en>
- LogRhythm, https://logrhythm.com/pdfs/infographics/IG_602_RansomwareGuide_Infographic_May16.pdf
- Tripwire, <http://www.tripwire.com/state-of-security/security-data-protection/using-the-nist-cybersecurity-framework-to-combat-ransomware-attempts/>
- Sophos, http://www.bankinfosecurity.com/whitepapers.php?wp_id=2685&user_email=james.dean@truecourseadvisory.com&rf=2016-08-08&mkt_tok=eyJpIjoiTTJGaE5tTTVZVFJoVVdRNCIsInQiOiJKKeksZMmxpT0RFSIwvM0ttSXpnODRUy0VsMmk4YWxDemJTZmNROHhUdG1CRFIVQ0R2RDlkTFo1MVBBOFhTZTNLTUVuVXRIQTRUZUNcL1V6aU1ZYjM2emlYVEV2RVwvd3pUVGplUmFDR2E4dHoyTT0ifQ%3D%3D

All judgments and assessments are solely based on unclassified sources and are the product of joint public and USG efforts.

