Ransomware and Other Cyber Extortion:

Preventing and mitigating increasingly targeted attacks

July 2016

digital shadows_

Executive Summary

Extortion is not new – it is simply the practice of obtaining something, often money, through force or threats.[1] Cyber extortion, which extends this criminal activity into the digital world, also isn't new, dating back to the early 1970s.[2] What is new, however, is the increase in the frequency of reported cases, likely fuelled by media coverage and new innovations.

Three main tactics are behind cyber extortion: the threat of distributed denial of service (DDoS), the threat of data compromise and ransomware. Actors such as DD4BC (DDoS for Bitcoin), the Armada Collective and Kadyrovtsy have all become notorious for these very tactics. Especially for organizations whose websites are revenue generating, these actors can cause enormous problems and their attacks can be very costly. With all of these actors, tools and variants, it is of little surprise that organizations are becoming increasingly concerned with the growing profile of cyber extortion.

But there can be benefits to this surge in reporting of extortion actors. There is plenty that organizations can learn about the actors involved and their tactics, tools and motivations. With this knowledge they can more effectively align their defenses and make better decisions in the face of an attack. Ransomware, however, is an ever-evolving threat that requires more than awareness to address. It requires a combination of technical and process controls and company-wide engagement – from employees, to executives, to IT security teams. This white paper provides insights into the tactics behind cyber extortion and key steps organizations can take to both prevent and mitigate the effects of increasingly targeted, profit-driven attacks.

Table of Contents

Cyber extortion: An introduction

Extortion is the practice of obtaining something, especially money, through force or threats. This is nothing new. If you are a fan of mafia shows then you are versed in the world of extortion. Whether it was paying off Tony Soprano in "The Sopranos" or Paulie Cicero in "Goodfellas," the bad guys get their money. Cyber extortion is the digital version of what "wise guys" have been doing for centuries. What is new, however, is the wide variety of methods that are used to achieve this. Staying up-to-date with the latest trends and innovation can be hard, but it is essential in order to effectively prevent and mitigate the effects of extortion on your business.

Since 2015, cyber extortion has become a hot topic in the mainstream media.[3] This is due in large part to the high profile of the group known as DD4BC, a group that targeted organizations that had revenue-generating websites. The group would ask organizations to pay a ransom in order to avoid a distributed denial of service (DDoS) attack against their website. Today, extortion extends beyond DDoS to include data. There are a number of instances where threat actors have used stolen sensitive, proprietary or confidential data as a means to extort affected individuals and organizations. Furthermore, new ransomware variants have emerged and continue to evolve to cause even more headaches for organizations. Verizon's 2016 Data Breach Investigations Report found vast increases in cases of ransomware.[4] With extortion continuing to be a popular method of attack, gaining an understanding of these various tools, actors and motivations allows organizations to better thwart these attacks.

DDoS-based extortion threats

One of the most popular means to facilitate extortion is through DDoS attacks. These types of attacks typically target business-critical websites in order to increase the likelihood of payment and can have crippling effects on organizations. Take the example of Code Spaces, an organization that went out of business as a result of not submitting to a DDoS extortion attempt.[5] One particularly well-known actor in this space is DD4BC, a group that was active between July 2014 and January 2016. Their three-stage process was typical and is used by most DDoS-based extortion actors:

1. An email, in which a sum of money is demanded, is sent to a targeted company or organization.
2. Payment is demanded to a Bitcoin (BTC) address, in order to avert the threat of a sustained DDoS attack that would impact the targeted organization's ability to generate revenue.
3. In some instances, such as when targeting hosting providers, the threat actor adds pressure to pay by using the negative publicity associated with service downtime as a threat.

Figure 1 - Typical stages of DDoS extortion.

The specific tactics and tools used by the group have included DDoS attacks that use SYN (synchronization packets) flood, NTP (Network Time Protocol servers) amplification, WordPress amplification, SSDP (Simple Service Discovery Protocol) amplification and UDP (User Datagram Protocol packets) flood. According to some reports, if the website was protected by DDoS protection then DD4BC attempted to target other infrastructure within the same data center in an effort to take the entire data center offline.[6] Evident from emails to victims, ransom requests from this group have ranged from as low as 1 to 100 BTC ($450 to $45,730).

With reports of the arrest and detainment of two individuals suspected of being associated with DD4BC in January 2016, it is likely that this threat actor is no longer active. But that doesn't signal the end of DDoS-based extortion. Two other groups, Armada Collective and Kadyrovsty, are also notable for their use of this tactic.

Armada Collective

Armada Collective is a threat actor that used the threat of DDoS attacks in an attempt to extort BTC from targeted companies, individuals and organizations. Armada Collective activity was first reported in September 2015 and continued until December 2015, targeting financial services, hosting providers, email providers and casinos. Armada Collective is known to have successfully extorted ProtonMail (an encrypted email service provider).

The Swiss Computer Emergency Response Team (CERT) reported that Armada Collective used different types of DDoS attacks as part of their targeting, namely DNS, NTP, SSDP and CHARGEN (Character Generator Protocol) amplification and reflection attacks.[7] The largest reported attack detected as part of Armada Collective activity flooded its victim with 772Mbps of traffic. Previous targeting conducted by Armada Collective has included ransom demands of between 10 and 200 BTC.

In March 2016, reporting of Armada Collective activity re-emerged. The threat actor was reported to have targeted an unknown number of financial institutions in Switzerland. The affected institutions are reported to have received emails that contained similar content to emails previously sent between September and December 2015. However, the email disclosed by Swiss CERT did not include a statement by the threat actor claiming that a demonstration attack would occur. There were also clear differences in the email addresses used. Based on the information provided by Swiss CERT, it is a realistic possibility that the more recently reported Armada Collective activity was conducted by a copycat actor seeking to capitalize on the previous successes of Armada Collective. This is further demonstrated by the absence of a demonstration attack or any other proof of capability.

Kadyrovtsy

Most recently, the Polish language security blog "Zaufana Trzecia Strona"[8] referred to a new actor named Kadyrovtsy, which it claims has used DDoS extortion to target banks and financial services firms in Poland and the UK. The approach described in this blog is consistent with that of a DDoS extortionist actor and is similar to activity previously linked with other extortionist actors such as DD4BC and the Armada Collective. The reported launch of DDoS attacks, ranging in volume from 40Gbps to 90Gbps, indicates a relatively high level of capability considering that attacks linked with DD4BC and Armada Collective have peaked at approximately 60Gbps. The demanded ransom of 20 BTC is relatively high for an actor of this type and the reported targeting of three Polish banks within a period of a few days potentially indicates high intent. Additionally, the use of a non-traceable email address not linked to any other online entities indicates an awareness of operational security practices. (You can read more about operational security in our recent whitepaper.[9])

The most common type of DDoS attack, volumetric DDoS extortion attempts, have benefited from low technical barriers, particularly the ease of access to so-called "booter" or "stresser" websites. These websites offer DDoS as-a-service and promise that cybercriminals with low technical knowledge can launch moderately powerful levels of attack. Two of the most popular examples of these tools are Shenron and Bangstresser. Methods employed as part of DDoS-based extortion, however, have remained the same in the past year and it is likely that threat actors employing DDoS-based extortion will continue to use similar tactics to those observed as part of Armada Collective and DD4BC activity.

Compromised data release and extortion

A second method of extortion involves the potential release of compromised data. This method is dependent on the fact that the target's data has already been compromised. The threat of its release to the public domain is used as blackmail in order to extort money from the affected entity. This tactic is not new.

A group called "Rex Mundi" emerged in May 2012 and allegedly compromised the databases of a number of companies based in French-speaking countries using this very approach.[10] Generally, Rex Mundi notifies the victims of the breach via social media and threatens to make the data public unless a ransom is paid within a given timeframe. In the past, most of the group's claims were assessed to have been legitimate.[11] More recently, there are three notable threat actors that have entered the fray: Hacker Buba, Poseidon Group and Russian Guardians.

Hacker Buba

On November 25, 2015, it was reported that an actor called "Hacker Buba" claimed to have stolen data from a Middle Eastern bank, Invest Bank. Hacker Buba threatened to release confidential customer and client information via various Twitter accounts, in an attempt to extort the bank for what was reported to be $3 million. One Twitter account associated with this activity posted on November 26, 2015, and claimed that they would sell databases of "all financial info" of clients including "credit card" information. The account also claimed they had "~900 gigs" of information. While the bank had confirmed a data breach had occurred, they claimed that they would not pay the ransom. Data subsequently emerged online, which included sensitive information of around 40,000 customers, including full names, credit card numbers and dates of birth. It was not known whether the data had legitimately been acquired from the bank, or how this was achieved.

Poseidon Group

A Portuguese-speaking threat actor called "Poseidon Group" was first discovered in 2015 but was reported to have been active since at least 2005.[12] The group allegedly targeted financial institutions, governments, public relations, manufacturing and natural resource companies in Brazil, the United States, France, Russia, Kazakhstan, India and the United Arab Emirates. The group is reported to have targeted proprietary information, technologies and business-sensitive information that represented value to investments and stock valuations. The actor stole intellectual property and commercial information, occasionally focusing on the personal information of executives. As part of campaigns, the group used extortion methods whereby it would threaten to disclose proprietary information in order to blackmail victim companies into contracting the Poseidon Group as a security firm.

Russian Guardians

The threat actor "Russian Guardians" is known to have compromised a number of external-facing servers in order to delete or steal any virtual machines (VMs) contained on the server. The group's campaign actions unfold in the following sequence:

1. Break into a server;
2. Delete or steal the VMs contained on the server;
3. Leave a folder or folders named "-HACKED-";
4. Leave a text file inside the folder containing an extortion message.

The messages, which vary only slightly, claim that the VMs have been stolen and are safely kept on the attackers' systems. In order to return the VMs, the attackers require a payment in BTC to a specified BTC wallet. The attackers offer two means of returning the data, either physically sending a Hard Drive Disk (HDD) or via an FTP server. If payment is not made, the attackers claim that the data will be sold to other criminals for further exploitation.

One common trend among victims is the use of ESXi server management software, likely due to its popularity. We deem it unlikely that zero days or other ESXi software-specific vulnerabilities were leveraged to execute the attacks. Additionally, each of the known attacks used a different BTC wallet. This, in conjunction with using complex transaction patterns passing BTC through hundreds of different wallets, likely obfuscate and complicate investigations. Nonetheless, a number of high value wallets that may be related to Russian Guardians have been found, including wallets with BTC valued at more than $315,000 or £200,000.

Given the fact that remotely downloading large VM files would be very time-consuming, it is probable that the attackers simply deleted the VMs instead of downloading them. However, if the VMs were in fact downloaded, the attackers may still be able to sell them for further profit. As a result, at this point it is unknown whether paying the ransom to the attacker will result in the actual return of the data.

Ransomware

The final type of extortion is ransomware, malicious software (malware) that restricts access to the computer system it has infected. The malware demands that a ransom be paid before restoring access to affected resources. Ransomware can prevent access to many features of a victim's machine, including files, applications and the operating system itself. Over the last six months Digital Shadows has increasingly reported on new ransomware variants and new techniques used by both the developers and operators of ransomware, including delivery methods, encryption methods and ransom payment methods.

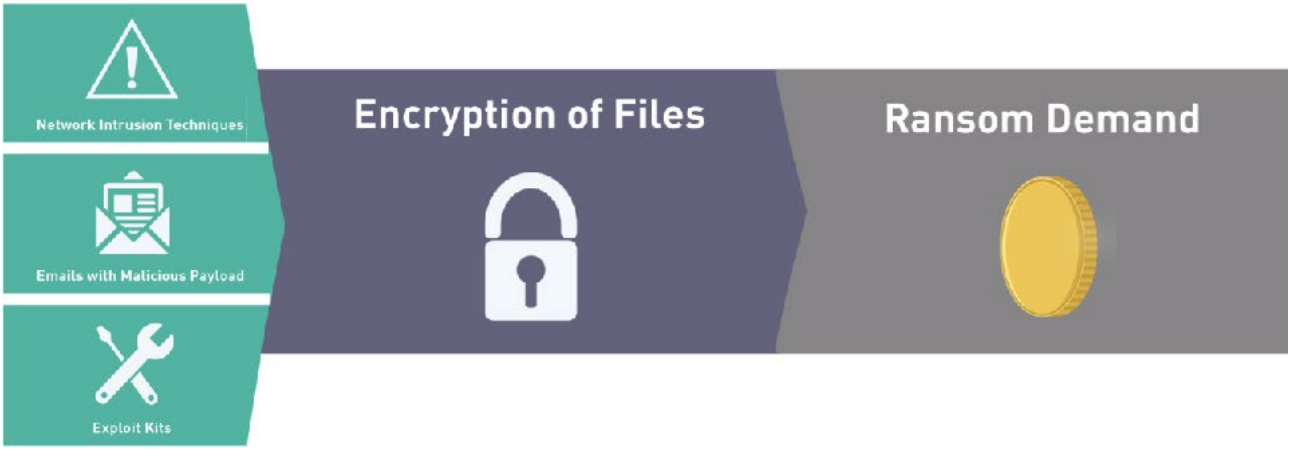

Figure 2 - Typical ransomware processes.

At a high-level, the ransomware process is fairly standard. Files are encrypted and the attackers, who hold the decryption key, will only allow the target to decrypt the files after the required BTC ransom is paid. Specific details of the attack, however, will depend on the variant. Here, we have selected five prevalent types of ransomware to examine more closely: Locky, Cerber, CryptoWall, SamSam and CryptXXX. Figure 3 compares these variants, including their infection methods, evidence of campaigns, encryption techniques, proliferation and ransom demands. There are, of course, far more than these five. Up until recently, for example, TeslaCrypt was a prevalent ransomware variant, though it's influence has understandably diminished following the release of the master decryption key.[13]

Variant	Locky	Cerber	Cryptowall	SamSam	CryptXXX
Infection methods observed	Exploit kit[14],[15] (Magnitude, Nuclear) Spam emails[16]	Exploit kit[17] (Magnitude) Compromised website	Spear-phishing emails[18] Spam emails[19] Exploit kits[20] (Angler[21], Magnitude[22], Neutrino[23], Nuclear[24])	Exploitation of unpatched vulnerabilities in external-facing servers[25]	Exploit kit (Angler, Neutrino)[26]
Evidence of targeted / untargeted campaigns	**Semi-targeted** Spam emails using a fake invoice as a social engineering lure[27]	**Untargeted** Mass infection of victims	**Untargeted to highly targeted** Spear-phishing emails to company executives with names and job titles[28] Small to medium businesses - email lures relating to resumes, orders and passport copies[29]	**Highly targeted** Network intrusion techniques employed (vulnerable JBoss application servers)	**Untargeted** Mass infection of victims
Encryption techniques (latest)	RSA-2048 and AES-128[30]	AES-256[31]	AES 256 CBC and RSA-2048[32]	Rijndael and RSA-2048[33]	RSA4096
Action	Encrypts local and mounted or networked drives[34]	Encrypts networked devices and files[35]	Encrypts local and mounted or networked drives[36]	Lateral movement by threat actor on the network	Encrypts files and harvests information and credentials
Ransom demands	approx. $220 - $1770[37][38]	approx. $500[39]	approx. $200 - $10,000[40]	approx. $440 - $750 per machine	approx. $500 - $1000

Figure 3 - Comparison of significant ransomware variants (see endnotes for references).

The relationship between the development of ransomware and decryption tools is a cat and mouse game; as quickly as a new decryption tool is released, the ransomware is updated. CryptXXX is a great example of this, a variant that is now up to version 3.100.[41]

Increasingly targeted delivery

Prior to March 2016, public reporting of ransomware infections suggested that multiple variants were typically delivered via drive-by-downloads from exploit kits, or through spam emails that either contained malicious attachments or encouraged recipients to visit websites hosting malicious content. Magnitude and Nuclear exploits kits were frequently associated with the delivery of a number of variants of ransomware, in addition to spam emails.

Technically, there are no barriers to actors targeting their ransomware infections towards specific victims. However, there may be some financial disincentives. Similar to other financially-motivated pursuits, actors must estimate their return on investment (ROI), in this case based on the likelihood of successful infection and payment of the ransom fee. The majority of publicly-reported ransomware campaigns have operated on the basis of high volumes of attempted infections and relatively low ransom demands. The hope is that even a small percentage of victims will pay, which in aggregate represents a significant profit to the attackers. Typical demands in 2015 were approximately $500,[42] although more recent attacks have demanded as much as $16,800.[43]

There have been a number of indicators to suggest that threat actors have started to use more targeted methods to affect organizations, as well as traditional, high volume approaches. While exploit kits and spam phishing emails will continue to be popular delivery methods for ransomware, evidence suggests delivery methods have widened in scope. Below are methods used by some significant ransomware variants for even more targeted delivery:

- Locky – delivered via spam emails purporting to include invoices. This subject matter was assessed to be relevant more to organizations than individuals, however it would likely lure individuals as well.
- SamSam – delivered through public-facing, vulnerable JBoss application servers used to pivot into internal networks. This is one of the most targeted approaches to ransomware delivery – alongside spear-phishing – that likely pertained to organizations rather than individuals.
- Rokku – while not a variant of ransomware that is a focus for this paper, Rokku is reported to have been delivered via phishing emails purporting to be from a job applicant. This suggests it is highly likely that organizations, as opposed to individuals, were targeted.
- CryptoWall – has been delivered via spear-phishing emails that included the name, job title and job-relevant information of the recipient. This, like SamSam, is evidence of a highly targeted approach to the delivery of ransomware.

New innovations, new opportunities

It is not only through increased targeting that ransomware actors have evolved. The recent media hype around ransomware, combined with reports of successful extortion, has fueled new innovation in ransomware. As shown in Figure 4, our dark web spider recently revealed a Tor hidden service calling itself the "Hall of Ransom."[44] The site advertised a number of services related to ransomware including the apparently multi-functional "Goliath" malware, which was offered for $2,100, payable in BTC of course. The advertisements claimed that the malware was based on the well-known Locky ransomware and included both ransomware and remote access functionality, allowing users to either download or lock the contents of their victims' machines. Goliath, it was claimed, was aimed at beginners with low technical understanding. The same site also offered access to Locky and a decrypter tool, which would be mailed on a USB stick to anyone for $1,200.

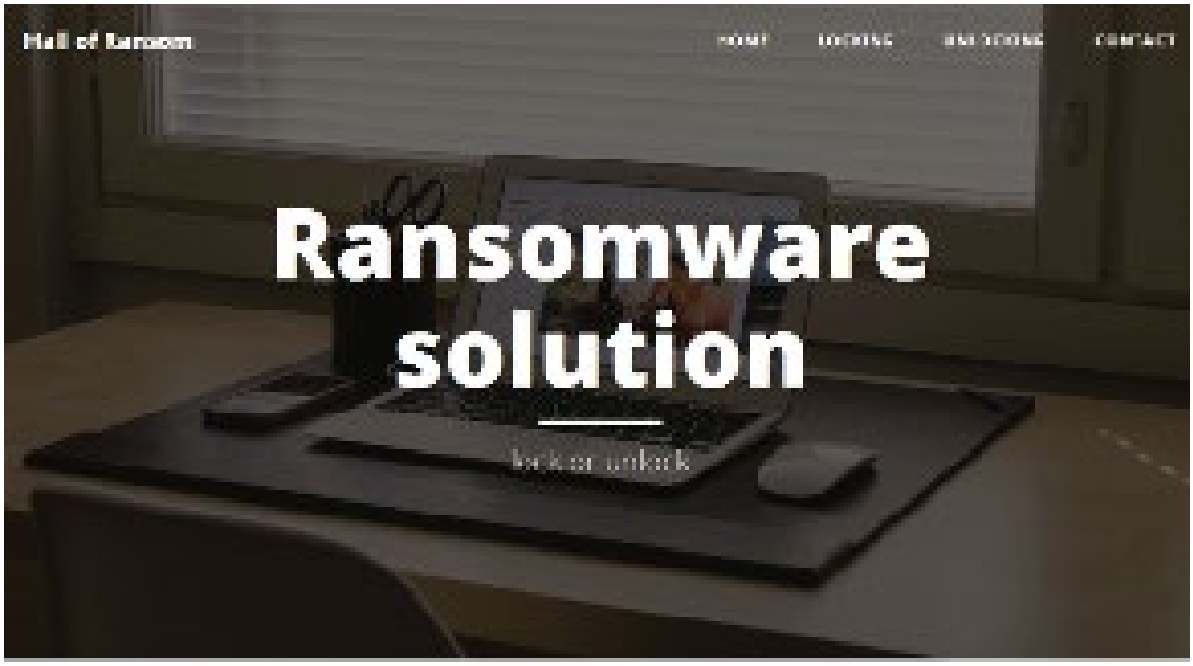

Figure 4 - An advertisement for "Goliath" by Hall of Ransom, claimed to be developed from the "Locky" variant.

Goliath ransomware is not the only variant to attempt to capitalize on the success of Locky. More recently, Zepto ransomware was reported to have been a version of Locky ransomware that appended encrypted files with ".zepto" and was delivered through spam emails containing a malicious JavaScript file..[45]

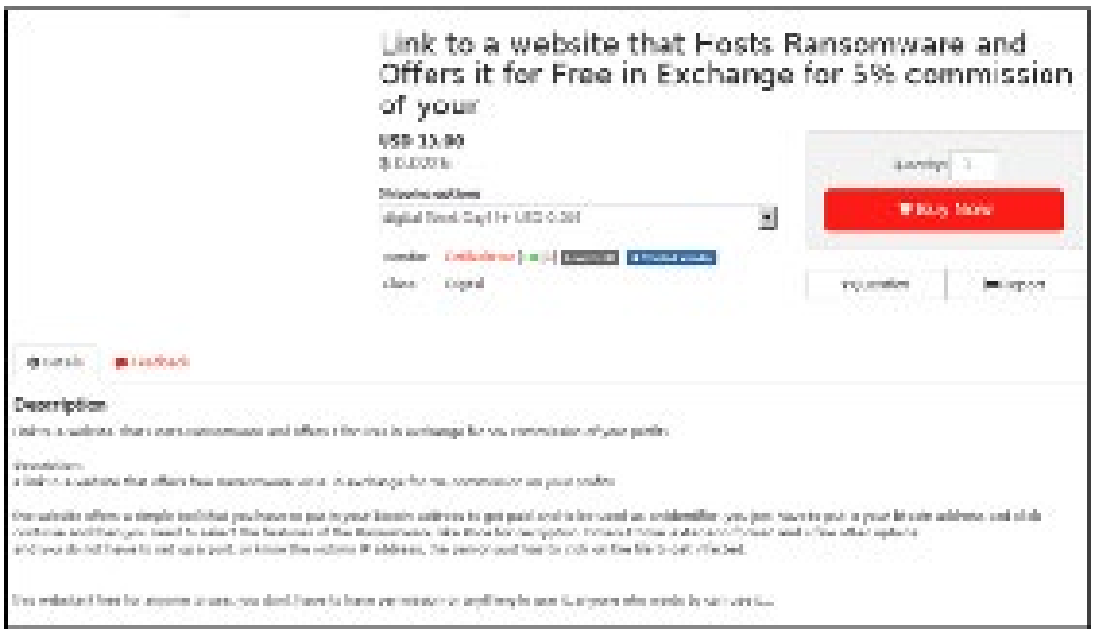

Figure 5 - A vendor offering a service that will host ransomware on your behalf, in return for 5 percent commission on the ransom payments received.

Another way to profit from ransomware is shown in Figure 5. On the Hansa marketplace, one seller offers a service that will host ransomware on a user's behalf, in return for 5 percent commission on the ransom payments received. While the possibility remains that these examples are merely scams, it points to the wide variety of opportunities that have opened up in 2016 with regards to ransomware and highlights the ever-increasing move towards greater ease of use and accessibility for the less technology savvy.

This activity demonstrates that the threat from ransomware is particularly prominent, given the increasingly frequent reporting of new variants employing new techniques. This has been further aided by the continued public reporting of attacks and, in some cases, the disclosure that organizations have paid the fee to unencrypt data. There is also increasing evidence that these attacks are becoming more targeted towards organizations. In order for their schemes to remain profitable, attackers continue to overcome the decryption tools and techniques that researchers develop. We assess that attackers, motivated by the potential for profits, will continue to develop ransomware techniques and variants in the near future.

Protecting your organization

In the past year, Digital Shadows has observed a considerable number of publicly-reported extortion attempts by attackers, using DDoS-based extortion, compromised data release extortion and ransomware to achieve their goals. It is highly likely the various forms of extortion will continue to present threats to organizations, companies and individuals in the foreseeable future.

By gaining an awareness of the tools and processes used by actors that employ DDoS-based extortion and compromised data release extortion, organizations are able to better align their defenses. Advanced knowledge of the typical demands of a threat actor and their capabilities is valuable to organizations that need to make complex decisions if presented with such a scenario.

Mitigating ransomware threats is more complex. The preventative advice includes understanding the infection vectors of the malware and applying the appropriate security controls to mitigate the risk of infection. This includes raising staff awareness of how ransomware attacks occur and the introduction of technical and procedural controls to prevent infection. Organizations are advised to develop ransomware planning procedures in the case of infection and to ensure that backups are maintained and are separate from the network.

Best practice for the prevention of ransomware infections includes a combination of technical and process controls, described in Appendix 1. If organizations do become victim to a ransomware infection, measures can be implemented in order to minimize impacts associated with infection. In addition, several decryption tools have been released, although the effectiveness of these tends to be short-lived as ransomware developers seek to evade them by developing their encryption methods. The prevention considerations below are largely referenced from an FBI advisory (available on request).

Authors: Rick Holland, Mark Tibbs, Simon Tame, Michael Marriott

Appendix 1: Prevention and mitigation advice for ransomware

Organizations should provide awareness and training for staff that may be targeted by ransomware. Staff should be made aware of the threat of ransomware, how it is delivered and information security principles and techniques. Channels should be open for staff to easily report suspected phishing attempts and to get validation prior to opening suspect mails and files. Additional details on preventing and mitigating such attacks are provided below. Much of this advice can be found in the FBI's tip for dealing with ransomware.[46]

Prevention	Mitigation
Ensure operating systems, software and firmware on devices is kept patched and updated as vulnerabilities are discovered. A centralized patch management system may facilitate this process.	Regularly backup data and verify its integrity.
Ensure anti-virus (AV) software is installed on end-points and kept regularly updated and scans are carried out regularly. Most AV solutions can be set to automatically update and scan.	Ensure that backups are remote from the main corporate network and machines they are backing up.
Provide awareness and training for staff that may be the end users targeted by ransomware. Staff should be made aware of the threat of ransomware (and malware in general), how it is delivered and information security principles and techniques. Open channels for staff to be able to report suspected phishing attempts. This should be a way for users to openly and easily report suspect emails and files to get validation prior to opening.	Use cloud-based or physical backups. Some ransomware can encrypt data on cloud-based backups when systems continuously back up in real time (persistent synchronization).
Manage the use of privileged accounts and ensure the "principal of least privilege" is implemented. Administrative access should be reserved only for those who require this. Those employees should only use the accounts when required and use regular user accounts for daily tasks.	While backups have long been seen as a way around paying out ransomware, targeting backup systems and slowly corrupting data may soon be a reality. Ensure you have a proper backup program in place that is being followed. Ransomware has been known to attack other systems on the network, and may soon specifically look for backup servers as a means to force users to pay instead of restoring from backups.
The principle of least privilege should also be implemented for file, directory and network share permissions. Users should not be given write access unless required.	Implement application whitelisting governed by a security policy which only allows the execution of a prescribed set of programs.
Disable macro scripts from Microsoft Office files transmitted via e-mail. Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full Office suite applications.	Use VMs for operating system environments of specific programs.
Implement software restriction policies (SRP) or other controls to prevent the running of executables in locations commonly used by ransomware, such as temporary folders supporting Internet browsers, or compression/decompression programs, including those located in the AppData/LocalAppData folder.	Data can be categorized based on organizational value and then physical or logical separation of networks can be created for different business functions (i.e., separating intellectual property from email systems).

End notes

1. Oxford English Dictionary, "Extortion".

2. Thomas Whiteside, Computer Capers: Tales of Electronic Thievery, Embezzlement & Fraud, (1978)

3. https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise

4. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

5. http://www.scmagazine.com/code-spaces-shuts-down-following-ddos-extortion-deletion-of-sensitive-data/article/356774/

6. www[.]youtube[.]com/watch?v=JK5TXl9jtNM (YouTube Video)

7. http://www[.]govcert.admin[.]ch/blog/15/update-on-armada-collective-extort-swiss-hosting-providers

8. https://zaufanatrzeciastrona[.]pl/post/niebezpiecznie-duzy-atak-ddos-na-polskie-banki-wraz-z-proba-szantazu/

9. http://info.digitalshadows.com/OPSECOpportunity-BlogAd_Registration.html

10. http://www.scmagazineuk.com/rex-mundi-how-did-dominos-incident-response-line-up/article/356549/

11. http://www.bloomberg.com/news/articles/2015-01-09/hackers-demand-12-000-for-client-data-stolen-from-geneva-bank

12. https://securelist[.]com/blog/research/73673/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/

13. http://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key/

14. http://blog[.]checkpoint[.]com/2016/04/11/new-locky-variant-implements-evasion-techniques/

15. http://blog.trendmicro[.]com/trendlabs-security-intelligence/cve-2016-1019-zero-day-integrated-in-exploit-kit/

16. https://www[.]trustwave[.]com/Resources/SpiderLabs-Blog/Massive-Volume-of-Ransomware-Downloaders-being-Spammed/?page=1&year=0&month=0

17. https://blog.malwarebytes.org/cybercrime/2016/04/magnitude-ek-malvertising-campaign-adds-fingerprinting-gate/

18. https://www[.]proofpoint[.]com/us/threat-insight/post/phish-scales-malicious-actor-target-execs

19. https://isc.sans[.]edu/diary/BizCN+gate+actor+sends+CryptoWall+4.0/20409

20. http://blogs.cisco[.]com/security/talos/cryptowall-3-0

21. https://threatpost[.]com/cryptowall-3-0-infections-spike-from-angler-ek-malicious-spam-campaigns/
22. http://malware.dontneedcoffee[.]com/2015/06/cve-2015-3113-flash-up-to-1800160-and.html
23. https://blog.malwarebytes[.]org/malvertising-2/2015/10/malvertising-campaign-targets-top-spanish-torrent-sites/
24. https://isc.sans[.]edu/diary/BizCN+gate+actor+sends+CryptoWall+4.0/20409
25. http://blog.talosintel[.]com/2016/03/samsam-ransomware.html
26. https://www.proofpoint.com/uk/threat-insight/post/cryptxxx-new-ransomware-actors-behind-reveton-dropping-angler
27. https://nakedsecurity[.]sophos[.]com/2016/02/17/locky-ransomware-what-you-need-to-know/
28. https://www[.]proofpoint[.]com/us/threat-insight/post/phish-scales-malicious-actor-target-execs
29. http://blog.trendmicro[.]com/trendlabs-security-intelligence/businesses-held-for-ransom-torrentlocker-and-cryptowall-change-tactics/
30. https://nakedsecurity[.]sophos[.]com/2016/02/17/locky-ransomware-what-you-need-to-know/
31. http://www.bleepingcomputer.com/news/security/the-cerber-ransomware-not-only-encrypts-your-data-but-also-speaks-to-you/
32. http://blog.talosintel[.]com/2015/12/cryptowall-4.html
33. http://blog.talosintel[.]com/2016/03/samsam-ransomware.html
34. https://nakedsecurity[.]sophos[.]com/2016/02/17/locky-ransomware-what-you-need-to-know/
35. http://www.bleepingcomputer.com/news/security/the-cerber-ransomware-not-only-encrypts-your-data-but-also-speaks-to-you/
36. http://www.bleepingcomputer[.]com/news/security/cryptowall-4-0-released-with-new-features-such-as-encrypted-file-names/
37. https://nakedsecurity[.]sophos[.]com/2016/02/17/locky-ransomware-what-you-need-to-know/
38. https://krebsonsecurity[.]com/2016/03/hospital-declares-internet-state-of-emergency-after-ransomware-infection/
39. http://blog.trendmicro.com/trendlabs-security-intelligence/cerber-crypto-ransomware-speaks-sold-russian-underground/
40. http://www.ic3.gov/media/2015/150623.aspx
41. https://www.proofpoint.com/us/threat-insight/post/cryptxxx-ransomware-learns-samba-other-new-tricks-with-version3100
42. http://www.havocscope [.]com/average-ransonware-demand-in-2015/

43. http://www[.]securityweek[.]com/hollywood-hospital-pays-17000-ransom-recover-files

44. http://www.digitalshadows.com/blog-and-research/goliath-ransomware-giant-problem-or-giant-con/

45. http://blog[.]talosintel[.]com/2016/06/gotta-be-swift-for-this-spam-campaign.html

46. https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise

About Digital Shadows

Digital Shadows provides insight into an organization's external digital risks and the threat actors targeting them. Digital Shadows SearchLight™ service combines scalable data analytics with human analysts to monitor for cyber threats, data leakage, and reputation risks. Digital Shadows continually monitors the Internet across the visible, deep and dark web, as well as other online sources to create an up-to-the minute view of an organization and provide it with tailored threat intelligence. The company is jointly headquartered in London and San Francisco. For more information, visit www.digitalshadows.com.

digitalshadows.com

London

Level 39, One Canada Square, London, E14 5AB

+44 (0) 203 393 7001 info@digitalshadows.com

San Francisco

332 Pine St. Suite 600, San Francisco, CA 94104

+1 (888) 889 4143

digital shadows_