2015

Ransomware: Emergence of the cyber-extortion menace

Nikolai Hampton
Edith Cowan University

Zubair A. Baig
Security Research Institute, Edith Cowan University

DOI: 10.4225/75/57b69aa9d938b
13th Australian Information Security Management Conference, held from the 30 November – 2 December, 2015 (pp. 47-56), Edith Cowan University Joondalup Campus, Perth, Western Australia.

RANSOMWARE: EMERGENCE OF THE CYBER-EXTORTION MENACE

Nikolai Hampton[1] Zubair A. Baig[2]
[1]School of Computer and Security Science, [2]Security Research Institute
Edith Cowan University, Perth, Australia
Email: {nikolaih, z.baig}@ecu.edu.au

Abstract

Ransomware is increasingly posing a threat to the security of information resources. Millions of dollars of monetary loss have been afflicted on end-users and corporations alike through unlawful deployment of ransomware. Through malware injection into end-user devices and subsequent extortion of their system or data, ransomware has emerged as a threat requiring immediate attention and containment by the cyber-security community. We conduct a detailed analysis of the steps of execution involved in ransomware deployment to facilitate readiness of the cyber-security community in containing the rapid proliferation of ransomware. This paper examines the evolution of malware over a period of 26 years and the emergence of ransomware in the cyber-threat landscape. Key findings on the evolution of ransomware and its use of emerging technologies are presented.

Keywords
malware; ransomware; ransom; security; cryptovirology; evolution; cyber security; computer security; bitcoin

A HISTORICAL INSIGHT

Cyber-extorting malware has been evolving for almost three decades. Whilst malware developers adopt new techniques to improve proliferation and evasion, security professionals respond reactively by playing catch-up. Zero-day attacks are thus rampant; frequent variations in malware signatures encumber the detection process and increase the level of risk that organisational networks face.

Cyber-extortion threats are not new, the widely reported PC CYBORG (AIDS) Trojan was the trendsetter in 1989. The strategies used by PC CYBORG are not too dissimilar to many new ransomware threats that have emerged over the last decade. PC CYBORG was delivered electronically via an infected floppy-disk, the installation used a dormancy period to evade users and authorities alike, which gave time for the malware to spread. It locked access to user files by encrypting the content and finally used a socially engineered message to claim the user was in 'breach of a licencing agreement' requiring it to pay $189 (via cheque posted to Panama) in order for a licence renewal (and decryption) disk to be sent.

Much of the malware activity in the 1990s was from hobbyist hackers determined to prove their technical prowess. It wasn't until the early 2000's that malware authors started to gain financial reaps directly and malware became a profiteering business. Most profits were generated from: direct information theft; creation of "botnets" for-hire; and advertising revenue (Bechtel, 2014). Malware authors also profited through theft of banking credentials or sensitive passwords (Condon, 2012); or they amassed networks of malware compromised machines constituting a network of bots and leased the network to the highest-bidders. Botnets had value because cyber criminals could use them to launch large-scale cyber-attacks against corporate targets, run phishing campaigns to steal credentials, or drop further malware that could scour users' hard drives for personal data and to assist in identity theft. Malware profits were dependent upon longevity i.e., persistence; by laying low and doing no obvious harm, malware could persist for long enough to steal information, spamming or powering botnets. The concept of extortion based malware – although present for over a decade – didn't take off as a financial model until around 2012.

Direct end-user extortion remained relatively unsophisticated until 2011; an era of "Fake AntiVirus" scams relied on social engineering techniques to trick naive users in to paying for non-existent virus removal tools. Many of these scams were eliminated by a crackdown on credit card payment facilities, the FakeAV threat dried up almost overnight (Krebs, 2011). Somewhat more complex malware used denial-of-service tactics to "lock" out a user from its system. These early "lockers" attacked the boot operations of a machine until a ransom was paid (Pantanilla, 2012). Because the file system content remained un-touched, security professionals rapidly adopted anti-virus recovery software to compensate. Although proposed by Young and Yung, 1996, the use of strong encryption to create "reversible denial of service attack[s]" didn't gain popularity until the first encrypting locker PGPCoder/GPCode was released in 2005 (Nazarov & Emelyanova, 2006a). GPCode represented the first

real world implementation of the schemes proposed by Young and Yung; encrypting disk content and demanding ransom payment. Many variants of GPCode contained flaws including poorly implemented encryption routines, insecure encryption keys, or poor file deletion strategies, which allowed recovery of deleted content; significantly however, GPCode continued to evolve, its deletion strategies became stronger and the encryption schemes and key lengths improved over time.

Even with the advent of encrypting lockers, malware authors did not immediately adopt the direct end-user ransom approach. Such type of extortion required many points of contact between the affected end-user, payment gateways and the malware profiteer, encumbering the success in extortion. Ransomware needed a 3rd party payment gateway provider to process payments; and it required direct communication with the attacker to prove ransom payment and "reverse" the attack. Malware remained profitable primarily through information and resource theft; direct end-user extortion still remaining too complicated and risky.

The perfect storm of ransomware needed three core technologies to align before it could become successful:

- Requirement for strong, reversible encryption to lock up a user's files,
- Dependence on a system for anonymously communicate keys and decryption tools, and
- Concealment i.e., setup of an untraceable way to pay the ransom.

The first ransomware to successfully combine these attributes was CTB-Locker; CTB standing for "Curve, TOR, and Bitcoin": elliptic curve cryptography provided fast secure encryption of file content. The Onion Routing (TOR) protocol allowed anonymous communication; and Bitcoin enabled secure, untraceable crypto-cash transactions. CTB-Locker was not without implementation flaws, however the business model made sense and within a very short period ransomware began to take off growing by 500% as reported in 2013 (Wood, 2014). Newer generations have started to spread to multiple platforms (BitDefender Labs, 2015; Kirk, 2015), seek out network shares and removable media; strategies that increase the reach of the technology, as well as reduce the effectiveness of network and external hard disk backups. If these traits prove to be effective, it is likely that new ransomware variants will improve upon them. While large corporate backup solutions currently offer protection against a wide range of threats, smaller organisations may not have sufficient financial or technical resources to institute strong backup procedures.

While the concept of direct end-user extortion is terrifying and hones great media coverage; Kharraz et al. (2015) suggest that ransomware may be relatively easily defeated. The authors noted that many ransomware samples contained flaws or performed actions, which could be detected. They suggested that stopping ransomware attacks might not be as difficult as it appears; however if history is to provide guidance, ransomware should not be dismissed as a passing fad.

This research shows ransomware's history of adapting to defensive strategies; it is only a matter of time until all current protections are inadequate. It is essential that security professionals actively analyse and predict the direction of ransomware development in order to pre-emptively develop secure technologies that protect end-users. Furthermore, the research shows the tenacity of ransomware developers; if the financial model evolves to a point where large corporate networks become viable targets, then they too will need to deal with ransomware threats.

Research design and method

The research sought to determine what features or ransomware have persisted over time. We addressed this question by identifying these so as to facilitate prediction of the direction to be taken by future generations of ransomware.

A survey was conducted on several major ransomware families. The goal was to formalise a nomenclature for ransomware traits and identify what new traits were emerging over time. Twenty-nine variants in nine families of frequently cited ransomware were identified from popular security and virus research blogs. Each ransomware was individually researched to determine a release date and what features or traits it exhibited.

Twenty-two "traits" (features) were selected for analysis (Table 1). These traits described the technical design of the ransomware from encryption technology through to payment options. The traits were selected based on features frequently described by the security research blogs in which they were identified.

Table 1 Ransomware selected for trait analysis

Name	Date	Sources
PC CYBORG	1989-12-19	(Smith, 2002)
One Half Virus	1994-10-31	(Trend Micro, 2000) (Hoffman, n.d.)
GPcode	2004-12-01	(Emm, 2008) (Nazarov & Emelyanova, 2006b)
GPCode.ac	2005-06-27	(F-Secure, 2005) (Nazarov, Gostev & Shevchenko, 2006) (Emm, 2008) (Nazarov & Emelyanova, 2006b)
GPCode.ad	2006-04-14	(Alan, 2006)
GPCode.ae	2006-06-02	(Alan, 2006) (Emm, 2008) (Nazarov & Emelyanova, 2006b)
GPCode.af	2006-06-06	(Alan, 2006) (Nazarov & Emelyanova, 2006b)
GPCode.af2	2006-06-06	(Waldron, 2006) (Nazarov & Emelyanova, 2006b)
GPCode.ag	2006-06-07	(Nazarov & Emelyanova, 2006b)
GPCode.ak	2008-06-05	(Keizer, 2008) (AO Kaspersky Lab, 2005) (Dunn, 2008) (Tromer, 2008)
GPCode.ax	2010-11-20	(Kamluk, 2010) (Lemos, 2010) (K, 2011)
GPCode.bn	2011-03-26	(Brulez, 2011)
Reveton.2012	2012-04-04	(Tikkanen & Karmina, 2012)
Cryptolocker	2013-05-09	(Emsisoft Labs, 2013) (Jarvis, 2013) (Bottomley, 2015)
Reveton.2013	2013-09-10	(Kujawa, 2013)
Reveton.XY	2013-10-22	(Horejsi, 2013)
CryptoLocker 2.0	2013-12-19	(Lipovsky, 2013) (Pichel, 2013) (Bottomley, 2015)
CryptoDefense	2014-03-26	(Symantec Security Response, 2014) (Abrams, 2014a)
CryptoDefense	2014-04-01	(Abrams, 2014a)
CryptoWall	2014-06-26	(Subramaniam, 2014) (Bottomley, 2015)
CTB-Locker	2014-07-15	(Kafeine, 2014) (Abrams, 2014b)
Reveton.2014	2014-08-19	(AVAST Software, 2014)
CryptoWall 2.0	2014-10-01	(Allievi & Carter, 2015b) (Olson, 2014) (Code 42 Software, 2015) (Bottomley, 2015)
CryptoWall 3.0	2015-01-14	(Allievi & Carter, 2015a) (Code 42 Software, 2015) (Bottomley, 2015)
Reveton.2015	2015-02-05	(Saarinen, 2015)
TeslaCrypt 0.2.5	2015-02-14	(Sinitsyn, 2015) (Bottomley, 2015)
TeslaCrypt 0.4.0	2015-02-14	(Sinitsyn, 2015) (Bottomley, 2015)
TeslaCrypt 2.0.0	2015-07-13	(Duncan, 2015) (Sinitsyn, 2015) (Bottomley, 2015)
TeslaCrypt 2.1	2015-09-07	(Abrams, 2015) (syntx, 2015) (BloodDolly, 2015) (Bottomley, 2015)

The list of traits identified for analysis is defined as follows in Table 2:

Table 2 Ransomware traits and benefits conferred

Abbreviation	Trait	Description
Encrypts	Encrypting	The ransomware encrypts user file content as opposed to simply "locking" access to the PC
Strng Cphr	Strong Cypher	The ransomware includes a strong and well implemented encryption cipher.
PKI	PKI	The use of PKI allows ransomware to encrypt content using a public key. The attacker controls the secret part of the key and is the only actor capable of decrypting the messages.
Autonomy	Autonomous	Autonomous destructive execution starts execution without the need to contact a C2 server. Variants that require C2 communications before their destructive routines start may be blocked by detecting network signatures.
DGA	DGA	Domain Generation Algorithms [DGA]s make take-downs of the C2 server more difficult. With static IP and domains, authorities can work with ISPs and domain registrars to block access to the offending servers. With a DGA, the server's host name is unpredictable, known only to the attacker.
HiddenTOR	TOR	Use of The Onion Routing [TOR] protocol provides a high degree of security and anonymity to the attackers and their servers.
HiddenI2P	I2P	Uses the Invisible Internet Project [12P] network for communication. Similar to the TOR network.
HideClient	Built in TOR/I2P Client	Anonymous network client built-in to the ransomware code. With a built in TOR or I2P clients, the encrypted "circuits" are created internally, the data leaving the infected machine is encrypted and the endpoints are concealed. This makes detection and mitigation significantly harder.
SecureEnc	Cryptographically Secure Data Encryption	The malware is theoretically secure i.e., the concepts employed are based on well known and studied cryptographic principles. Tried and tested cryptography is strong by design, the wider the distribution of the algorithms the more peer review and the stronger the cryptographic design.
SecureKeys	Cryptographically Secure Keys	The keys used for encryption are of sufficient length and type to make cracking the encrypted content impossible without the correct key.
SecKeyMgmt	Secure Key Management	Key management is core to cryptographic security, for symmetric cryptography the keys cannot be permitted to persist on the hard disk or in memory. When using PKI, the secrecy of the private-key is paramount to the security of the whole cryptosystem.
ScanNetDrv	Scans Network Drives	The destructive code scans for files on external and network drives. This can be especially destructive for business and corporate offices, it can also find and encrypt network backups
SecErase	Securely Erases Originals	Securely deletes the original "encrypted" version of the user's files. Without secure deletion and overwrite, it may be possible to recover file content from internal operating system "shadow copies" or using file recovery software.
PK DL	Public Key Download	By creating server-side secret keys and releasing only public keys for infected computers the encrypted data is protected. Infected users have no access to the secret key which makes decryption impossible.
DH-ECC	DH-ECC PKI	Diffie-Hellman Elliptic Curve Cryptography [DH-ECC] is used to generate public keys. DH-ECC is a new generation of fast and very secure public key algorithms.
C2 Server	Uses C2 Server	Communicates with a command and control [C2] server to provide information or receive processing data or instructions.
C2 Hidden	C2 on Hidden Network	Command and control takes place over anonymous networks. This makes takedowns of control servers more difficult as law enforcement and ISPs cannot identify traffic content, specific Internet hosts, or domains in use.
PayProcOK	Good Payment Protocols	The payment and verification protocol is secure; the ransomware has a reliable way of verifying payments. This also means that the payment verification cannot be faked or circumvented.
PayPrvider	Uses Semi-Anonymous Payment Authority	The malware uses an anonymous payment method. By using secure anonymous payments the attackers can receive their cash without leaving a "paper trail". All centralised payment processors leave some type of paper trail; however, different processors have different identity requirements for their clients.
CryptCash	Uses Crypto Currency	Crypto currencies like Bitcoin offer secure, irreversible transactions. These types of payments are equivalent to cash passed from one person to another. Some ransomware also steal Bitcoins directly from electronic wallets.
StealCred	Steals Credentials	Steals user login, banking or identity credentials in addition to ransom demand.
StealProc	Steals Processing	Uses the infected machine to perform computing or network operations in addition to ransom demand. This could include password cracking, Bitcoin

Abbreviation	Trait	Description
	Power	mining, operating as part of a bot-net, or sending spam.

A ransomware traits matrix (Table 3) was produced to show the inclusion of "secure" traits and how they evolved over time. The table includes the ransomware variant name, the approximate date it was first identified and an assessment to identify whether specific traits were present and how well they were implemented.

RESULTS

Ransomware samples with first-observed dates ranging from December 1989 to July 2015 were identified. Of the twenty-nine strains identified, over half (15) were released in the last two years. A clear increase in the rate of new ransomware variants can be observed from Figure 1.

Examining the traits of the ransomware shows that while the first encrypting ransomware was uncovered in 1989, the first use of strong cryptographic principles was not until 2013, at which time ransomware began using cryptographically secure encryption algorithms. Other significant improvements can be seen in the use of anonymous networks like TOR and I2P and the introduction of crypto currencies. The use of anonymous hidden networks first appeared in mid-2014 for payment verification; since then, three-quarters of the ransomware variants observed used some type of anonymising service to enable secure communication. Crypto currencies have also significantly impacted the ransomware threat landscape. Bitcoin was first used in 2013 by Cryptolocker and again, approximately three-quarters of ransomware variants have included support for crypto currencies.

The data shows the enhancements to ransomware as a malware tactic. A brief increase in the numbers of ransomware variants during 2006-2007 was due to the introduction of the first variants of GPCode. Since 2010, ransomware variants became even more prominent. Figure 1 shows that technologies including crypto currencies and anonymous hidden networks are relatively new on the scene. The uptake of cryptocurrencies has been significant between 2013 and 2015 and data regarding the use anonymous networks has just begun to emerge. Moreover, the use of the TOR anonymization protocol saw a significant increase 2014 onwards.

Table 3 Matrix of ransomware security traits for selected strains

Strain	Date	Encrypts	Strng Cphr	PKI	Autonomy	DGA	HiddenTOR	HiddenI2P	HideClient	SecureEnc	SecureKeys	SecKeyMgmt	ScanNetDrv	SecErase	PK DL	DH-ECC	C2 Server	C2 Hidden	PayProcOK	PayPrvider	CryptCash	StealCred	StealProc
PC CYBORG	1989-12-19	√			√																		
One Half Virus	1994-10-31	√			√																		
GPcode	2004-12-01	√			√															√			
GPCode.ac	2005-06-27	√		o	√					x	x	x								√			
GPCode.ad	2006-04-14	√		o	√					x	x	x								√			
GPCode.ae	2006-06-02	√		o	√					x	x	x								√			
GPCode.af	2006-06-06	√		o	√					x	x	x								√			
GPCode.af2	2006-06-06	√	x	o	√					x	x	x								√			
GPCode.ag	2006-06-07	√	x	√	√					x	√	x								√			
GPCode.ak	2008-06-05	√	x	√	√					o	o	o								√			
GPCode.ax	2010-11-20	√	√	√	√					√	√	√							o	√			
GPCode.bn	2011-03-26	√	√	√	√					√	√	x							o	√			
Reveton.2012	2012-04-04				√												o		o	√			
Cryptolocker	2013-05-09	√	√	√		o				√	√	√	√		√		√		o	√	√		
Reveton.2013	2013-09-10				√												o		o	√			√
Reveton.XY	2013-10-22				√												o		o	√			
CryptoLocker 2.0	2013-12-19	√	√	√						√	√	√	√		√		√		o		√		
CryptoDefense	2014-03-26	√	√	√			o			√	√	x					√	o					
CryptoDefense	2014-04-01	√	√	√			o			√	√	√		o			√	o					
CryptoWall	2014-06-26	√	√	√						√	√	√	o		√		o		o		√		
CTB-Locker	2014-07-15	√	√	√	o		o			√	√	√	o		√	√	√		o		√		
Reveton.2014	2014-08-19				√												√		o	√	o	√	√
CryptoWall 2.0	2014-10-01	√	√	√			o			√	√	√	o		√		√	√	√		√		
CryptoWall 3.0	2015-01-14	√	√	√				√		√	√	√	o		√		√	√	√		√		
Reveton.2015	2015-02-05				√												√		o	√	o	√	√
TeslaCrypt 0.2.5	2015-02-14	√	√				√			√	√	x					√	√	x		√		
TeslaCrypt 0.4.0	2015-02-14	√	√		o		√			√	√	o	√	√			√	o	√		√		
TeslaCrypt 2.0.0	2015-07-13	√	√	√	o		√			√	√	o	√	√		√	√	√	√		√		

Strain	Date	Encrypts	Strng Cphr	PKI	Autonomy	DGA	HiddenTOR	HiddenI2P	HideClient	SecureEnc	SecureKeys	SecKeyMgmt	ScanNetDrv	SecErase	PK DL	DH-ECC	C2 Server	C2 Hidden	PayProcOK	PayPrvider	CryptCash	StealCred	StealProc
TeslaCrypt 2.1	2015-09-07	√	√	√	o		√			√	√	√	√	√		√	√	√	√		√		
√ = well implemented; o = not fully implemented; x = implementation broken																							

A brief increase was noticed during 2006-2007 through introduction of first variants of GPCode, since 2010 ransomware variants become more prominent. Figure 1 shows that technologies including crypto currencies and anonymous hidden networks are relatively new on the scene. The uptake of crypto currencies has been significant between 2013 and 2015 and data regarding the use anonymous networks has just begun to emerge.

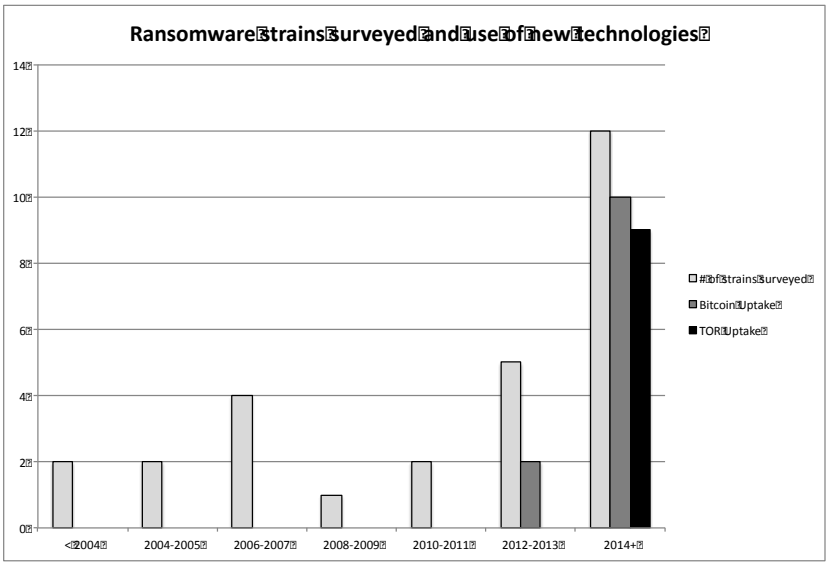

Figure 1 Increase in ransomware strains and security features identified over time

Another trend shows the increasing use of multiple security features and technologies; original ransomware variants were very simple by comparison. The data indicate that many current variants of ransomware have copied code and features from predecessors. An exception is a ransomware suite called Reveton, which has been through many revisions since 2012 and is still in circulation today, even with minor variations from one version to another. A closer examination of Reveton features indicate that it's "locking" performs no encryption it simply locks the "boot process" to interrupt standard PC operation.

DISCUSSION

The data show the general trend of ransomware to build on the technologies of previous generations. They also show that the encrypting ransomware is on the increase, each generation is building on the successes (and fixing the errors) of previous generations. In some cases as with early versions of GPCode, rapid iterations can be seen. Each new version of GPCode quickly plugged the holes and errors of the previous version. The result of these rapid updates was that GPCode became "unbreakable" in less than five years. The lessons learned and published vulnerability analysis has also taught other developers what GPCode did wrong; since GPCode.ax, no significant encrypting ransomware has utilised poor RSA key lengths or constructs.

The significant developments over time have been the addition of increasingly secure algorithms and key management methodologies. The evolutions have also shown a migration away from "home-brew" encryption routines to well established and proven cryptographic constructions. Most new secure variants of encrypting ransomware use a combination of: public key cryptography; >AES-256 block ciphers; remote public key generation; and C2 server communication.

One interesting variant that persists despite lacking any encryption features is Reveton. All variants perform locking operations based on interrupting the normal boot sequence. This attack is relatively easily circumvented and clean from an infected PC. A brief search through the literature on Reveton indicates that the locking component of the malware may be incidental to its other operations which include: password and credential stealing; Bitcoin mining (a legitimate process); and stealing of Bitcoin wallets (Kujawa, 2013) (Saarinen, 2015).

The ransom component apparently offers little benefit other than to frustrate user access to an infected PC while other malicious activities are taking place.

The recent emergence of TOR and I2P anonymous networks as a communication channel shows promise; logically, these encrypted and hidden networks provide malicious attackers another level of anonymity. There appears to be a general uptake of the technology, however the limited data makes it difficult to forecast future trends. It may be that TOR and I2P are too complicated for easy implementation; however, if other technologies are to provide any guidance, the learning experiences from each generation provide improved models for future developments.

One example of the rapid absorption of new technologies can be seen in the increasing use of the Bitcoin crypto currency as a payment method. This may be due to well-documented Bitcoin protocols and the widely publicised Bitcoin brand (Bitcoin Project, 2015). Implementation of Bitcoin payments requires very little overhead and may even be easier than clearing payments through conventional payment gateways and prepaid "debit" cards. The laundering and liquidation of Bitcoin assets is also a relatively straightforward process, with the protocol allowing "coins" to be combined and spilt arbitrarily. Traceability of Bitcoins is a field of active research (Reid & Harrigan, 2011), however the general user perception is that Bitcoin transactions are completely un-traceable; certainly they offer far greater anonymity than other online payment methods.

CONCLUSION

Through this paper we have presented a categorisation and an analysis of several key features of ransomware. In addition, we presented the evolution of ransomware over a period of twenty-six years. The environment of ransomware proliferation and its widespread and menacing threat landscape was also analysed.

Risks to corporate data are often mitigated through active security management, documented security policies, controlled access environments, skilled security personnel and enterprise firewalls and backup solutions. However, it is difficult to believe the technical or financial resources available to smaller organisations and individuals will be sufficient to protect against this rapidly evolving threat. The current state of malware research is very limited in contribution. Unlike vulnerability analysis – which is well documented in exploit databases – malware research and analysis is lacking peer-reviewed data resources and standardised analysis of malware development. Whilst malware analysis is conducted on an individual or a software manufacturer level, the opportunity exists to create a formal approach and vocabulary for convenient analysis of malware, variants and evolution.

REFERENCES

Abrams, L. (2014a, March). CryptoDefense and How_Decrypt Ransomware Information Guide and FAQ. Retrieved October 27, 2015, from http://www.bleepingcomputer. com/virus-removal/cryptodefense-ransomware-information

Abrams, L. (2014b, July). CTB Locker and Critroni Ransomware Information Guide and FAQ. Retrieved October 27, 2015, from http://www.bleepingcomputer.com/virusremoval/ctb-locker-ransomware-information

Abrams, L. (2015, October). Latest TeslaCrypt Ransomware adds the .ccc extension to Encrypted FIles. Retrieved October 28, 2015, from http://www.bleepingcomputer.com/ news / security / latest teslacrypt ransomware adds the ccc extension to encrypted files/

Alan. (2006, June). New GpCode ransom virus with a 660 bit key grc.security. Retrieved October 27, 2015, from http://codeverge.com/grc.security/new-gpcode-ransomvirus-with-a-660-bit-key/1660966

Allievi, A. & Carter, E. (2015a, February). Cryptowall 3.0: Back to the Basics. Retrieved August 25, 2015, from http://blogs.cisco.com/security/talos/cryptowall-3-0

Allievi, A. & Carter, E. (2015b, January). Ransomware on Steroids: Cryptowall 2.0. Retrieved August 25, 2015, from http://blogs.cisco.com/security/talos/cryptowall-2

AO Kaspersky Lab. (2005). Trojan-Ransom.Win32.Gpcode.ak. Retrieved October 28, 2015, from http://w.securelist.com/en/descriptions/Trojan-Ransom.Win32.Gpcode.ak

AVAST Software. (2014, August). Avast blog Reveton ransomware has dangerously evolved. Retrieved October 27, 2015, from https://blog.avast.com/2014/08/19/revetonransomware-has-dangerously-evolved/

Bechtel, K. (2014, March). Malware's Journey from Hobby to Profit-Driven Attacks. Retrieved October 8, 2015, from http://www.tenable.com/blog/malware-s-journeyfrom-hobby-to-profit-driven-attacks

Bitcoin Project. (2015). Developer Reference Bitcoin. Retrieved October 27, 2015, from https://bitcoin.org/en/developer-reference

BitDefender Labs. (2015). Linux Ransomware Debut Fails on Predictable Encryption Key | Bitdefender Labs. Retrieved from http://labs.bitdefender.com/2015/11/linux-ransomware-debut-fails-on-predictable-encryption-key/

BloodDolly. (2015, September). TeslaDecoder released to decrypt .EXX, .EZZ, .ECC files encrypted by TeslaCrypt Page 12 Archived News. Retrieved October 28, 2015, from http://www.bleepingcomputer.com/forums/t/576600/tesladecoder-released-todecrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/page-12

Bottomley, K. (2015, August). Tracking the Footprints of Ransomware. Retrieved October 28, 2015, from https://labs.opendns.com/2015/08/20/tracking-the-footprints-ofransomware/

Brulez, N. (2011, March). Ransomware: GPCode strikes back Securelist. Retrieved October 27, 2015, from https://securelist.com/blog/incidents/29784/ransomware-gpcodestrikes-back/

Code 42 Software. (2015). Recovering Files Infected By CryptoLocker Or CryptoWall. Retrieved October 27, 2015, from http://support.code42.com/CrashPlan/4/ Troubleshooting/Recovering_Files_Infected_By_CryptoLocker_Or_CryptoWall

Condon, C. (2012, May). StopTheHacker.com | How do cybercriminals profit from infecting websites with malware? Retrieved October 8, 2015, from http://www.stopthehacker.com / 2012 / 05 / 29 / how do cybercriminals profit from infecting websites with malware/

Duncan, B. (2015, July). Malware-Traffic-Analysis.net 2015-07-20 Nuclear EK sends TeslaCrypt 2.0. Retrieved October 28, 2015, from http://www.malware-traffic-analysis.net/2015/07/20/

Dunn, J. (2008-09-30T10:53-05:00). Police 'find' author of notorious Gpcode virus. Retrieved October 27, 2015, from http://www.infoworld.com/article/2653962/security/police-find--author-of-notorious-gpcode-virus.html

Emm, D. (2008, September). Cracking the code: The history of Gpcode. *Computer Fraud & Security*, *2008*(9), 15–17. doi:10.1016/S1361-3723(08)70139-8

Emsisoft Labs. (2013, September). CryptoLocker – a new ransomware variant. Retrieved October 27, 2015, from http://blog.emsisoft.com/2013/09/10/cryptolocker-a-new

ransomware-variant

F-Secure. (2005, May). Trojan: W32/Gpcode Description | F-Secure Labs. Retrieved October 27, 2015, from https://www.f-secure.com/v-descs/gpcode.shtml

Hoffman, P. (n.d.). Online VSUM One Half Virus. Retrieved October 28, 2015, from http://wiw.org/~meta/vsum/view.php?vir=994

Horejsi, J. (2013, October). Avast blog ˇ Win32:Reveton-XY [Trj] saves hundreds of computers worldwide and cybercriminals know it!!! Retrieved October 28, 2015, from https://blog.avast.com/2013/10/22/win32reveton-xy-trj-saves-hundreds-of-computers-worldwide-and-cybercriminals-know-it/

Jarvis, K. (2013, December). CryptoLocker Ransomware. Retrieved August 25, 2015, from http : / / www . secureworks . com / cyber -threat -intelligence / threats / cryptolocker -ransomware/

K, S. (2011, January). XyliBox: GpCode Ransomware 2010 Simple Analysis. Retrieved October 27, 2015, from http://www.xylibox.com/2011/01/gpcode-ransomware-2010-simple-analysis.html

Kafeine. (2014, July). "Crypto Ransomware" CTB-Locker (Critroni.A) on the rise | Malware don't need Coffee. Retrieved October 28, 2015, from http://malware.dontneedcoffee. com/2014/07/ctb-locker.html

Kamluk, V. (2010, November). GpCode-like Ransomware Is Back -Securelist. Retrieved October 27, 2015, from https://securelist.com/blog/research/29633/gpcode-like-ransomware-is-back/

Keizer, G. (2008, June). Security firm asks for help cracking ransomware key. Retrieved October 8, 2015, from http://www.computerworld.com/article/2535229/security0/ security-firm-asks-for-help-cracking-ransomware-key.html

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L. & Kirda, E. (2015). Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. In *Detection of Intrusions and Malware, and Vulnerability Assessment: 12th International Conference, DIMVA 2015, Milan, Italy, July 9-10, 2015, Proceedings* (Vol. 9148, p. 3). Milan, Italy: Springer.

Kirk, J. (2015, September 11). This nasty Android ransomware changes your phone's PIN code. Retrieved from http://www.pcworld.com/article/2983138/security/android-ransomware-changes-a-devices-pin-code.html

Krebs, B. (2011, August). Huge Decline in Fake AV Following Credit Card Processing Shakeup – Krebs on Security. Retrieved October 8, 2015, from http://krebsonsecurity. com/2011/08/huge-decline-in-fake-av-following-credit-card-processing-shakeup/

Kujawa, A. (2013, September). Ransomware Puts Your System To Work Mining Bitcoins. Retrieved October 27, 2015, from https://blog.malwarebytes.org/intelligence/2013/ 09/ransomware-puts-your-system-to-work-mining-bitcoins/

Lemos, R. (2010, December). Ransomware returns: 'If you ever want to see your data again...' | InfoWorld. Retrieved October 27, 2015, from http://www.infoworld.com/article/ 2624967/malware/ransomware-returns---if-you-ever-want-to-see-your-data-again----.html

Lipovsky, R. (2013, December). Cryptolocker 2.0 – new version, or copycat? Retrieved October 27, 2015, from http://www.welivesecurity.com/2013/12/19/cryptolocker-2-0-new-version-or-copycat/

Nazarov, D. & Emelyanova, O. (2006a, June). Blackmailer: the story of Gpcode -Securelist. Retrieved October 8, 2015, from https://securelist.com/analysis/publications/36089/ blackmailer-the-story-of-gpcode/

Nazarov, D. & Emelyanova, O. (2006b, June). Blackmailer: the story of Gpcode -Securelist. Retrieved October 8, 2015, from https://securelist.com/analysis/publications/36089/ blackmailer-the-story-of-gpcode/

Nazarov, D., Gostev, A. & Shevchenko, A. (2006, April). Malware Evolution: January -March 2006 -Securelist. Retrieved October 27, 2015, from https://securelist.com/ analysis/malware-evolution-monthly/36080/malware-evolution-january-march-2006/

Olson, R. (2014, October). Tracking New Ransomware CryptoWall 2.0 -Palo Alto Networks BlogPalo Alto Networks Blog. Retrieved October 27, 2015, from http://researchcenter. paloaltonetworks.com/2014/10/tracking-new-ransomware-cryptowall-2-0/

Pantanilla, C. (2012, April). Ransomware Takes MBR Hostage | Malware Blog | Trend Micro. Retrieved October 8, 2015, from http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-takes-mbr-hostage/

Pichel, A. (2013, December). New CryptoLocker Spreads Via Removable Drives | Security Intelligence Blog | Trend Micro. Retrieved October 27, 2015, from http://blog. trendmicro . com / trendlabs -security -intelligence / new -cryptolocker -spreads -via -removable-drives/

Reid, F. & Harrigan, M. (2011, July). An Analysis of Anonymity in the Bitcoin System. *arXiv:1107.4524 [physics]*. Retrieved October 27, 2015, from http://arxiv.org/abs/ 1107.4524

Saarinen, J. (2015, February). Extortionists upgrade Reveton ransomware. Retrieved October 27, 2015, from http://www.itnews.com.au/news/extortionists-upgrade-reveton-ransomware-400172

Sinitsyn, F. (2015, July). TeslaCrypt 2.0 disguised as CryptoWall -Securelist. Retrieved October 27, 2015, from https://securelist.com/blog/research/71371/teslacrypt-2-0-disguised-as-cryptowall/

Smith, G. (2002, August). The Original Anti-Piracy Hack. Retrieved October 8, 2015, from http://www.securityfocus.com/columnists/102

Subramaniam, S. (2014, July). CryptoWall Ransomware Built With RC4 Bricks. Retrieved October 28, 2015, from https://blogs.mcafee.com/mcafee-labs/cryptowall-ransomware-built-with-rc4-bricks/

Symantec Security Response. (2014, March). CryptoDefense, the CryptoLocker Imitator, Makes Over 34,000 in One Month. Retrieved October 27, 2015, from http://www. symantec . com / connect / blogs / cryptodefense -cryptolocker -imitator -makes -over -34000-one-month

syntx. (2015, October). @malware_traffic This one is actually #TeslaCrypt 2.1.0a. Wonder what's new, if anything... pic.twitter.com/L2AW6zZKT6. microblog. Retrieved October 28, 2015, from https://twitter.com/tehsyntx/status/657934762087157760

Tikkanen, A. & Karmina. (2012, April). Police Themed Ransomware Continues. Retrieved October 27, 2015, from https://www.f-secure.com/weblog/archives/00002344.html

Trend Micro. (2000, March). ONE_HALF.3544 -Threat Encyclopedia -Trend Micro US. Retrieved October 28, 2015, from http://www.trendmicro.com/vinfo/us/threatencyclopedia/archive/malware/one_half.3544

Tromer, E. (2008). Cryptanalysis of the Gpcode.ak ransomware virus. Retrieved October 27, 2015, from http://rump2008.cr.yp.to/6b53f0dad2c752ac2fd7cb80e8714a90.pdf

Waldron, H. (2006, June). Gpcode.af -Encrypts Pc Files And Holds User Hostage -General Security. Retrieved October 27, 2015, from http://www.bleepingcomputer.com/ forums/t/54683/gpcodeaf-encrypts-pc-files-and-holds-user-hostage/

Wood, P. (2014, July). Is Ransomware poised for growth? Retrieved October 8, 2015, from http://www.symantec.com/connect/blogs/ransomware-poised-growth

Young, A. & Yung, M. (1996). Cryptovirology: Extortion-Based Security Threats and Countermeasures. In *2014 IEEE Symposium on Security and Privacy* (p. 0129). Los Alamitos, CA, USA: IEEE. doi:10.1109/SECPRI.1996.502676