



Ransomware

Past, Present, and Future

Technical Marketing Team

Contents

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

4

Ransomware:
History and Evolution

7

2016: The Year Ransomware
Reigned

14

Ransomware:
Mitigation and Prevention

17

Appendix



Extortion is a cybercrime staple and no malware does a better job at this than ransomware.

Ransomware have been wreaking havoc since they first emerged in the mid-2000s. 2016 was, in fact, marked by a staggering increase the number of newly discovered ransomware families. All armed with capabilities to encrypt various file types on not just computers but even mobile devices and servers, individuals and businesses alike across the globe continued to suffer the threat's dire effects.

Ransomware operators not just improved the malware's capabilities but also produced increasingly threatening ransom notes while demanding bigger ransoms. Incidents have left victims no other choice but to give in to cybercriminals' demands just to get files back or worse their systems back up and running.

To this day, new and improved ransomware variants continue to be seen. Will we see the end of ransomware scare soon?

Ransomware: History and Evolution

The first cases of ransomware¹ infection were first seen in Russia between 2005 and 2006. One of our earliest reports on ransomware discussed a variant that compresses then password-protects certain files in a victim's computer.² It also left a file that served as ransom note to ask the victim for US\$300 in exchange for his files. In the threat's early stages, .DOC, .XLS, .JPG, .ZIP, .PDF, and other commonly used files were held hostage. Later on, variants that could infect mobile phones³ and even computers' Master Boot Record (MBR),⁴ preventing the OS from loading, emerged.

By 2012, ransomware made its way from Russia across other European countries.⁵ This could be a result of the clampdown on fake antivirus (FAKEAV) and so cybercriminals had to look for another means to continue profiting from unwitting victims.⁶ Ransomware operators started coming up with new tactics to spread the threat. A popular ruse at that time was introduced by Reveton⁷—impersonating law enforcement agencies and threatening victims by implicating them with online crimes. Ransomware operators also experimented with the use of various payment methods, including Ukash, paysafecard, and MoneyPak, to limit their monetary trail.



FAKEAV variants typically scare users into doling out cash with fake alerts touting computer infection

Early ransomware variants scared users with screen lockouts

Today's ransomware variants not only lock users out of their systems but also threaten to delete all of their files if they do not pay the ransom

Figure 1. From FAKEAV to ransomware

In late 2013, what we know now as “crypto-ransomware” led by variants like CryptoLocker⁸ came to the fore. This threat no longer just encrypted files, it started deleting files if victims refused to pay. To get files back, victims were asked to pay varying ransom amounts in the form of Bitcoins in exchange for a decryption key.

Since the introduction of crypto-ransomware, cybercriminals increasingly took steps to more effectively extort money from victims—individuals and businesses (regardless of size) alike from virtually any part of the world.

Delivery Means

Ransomware reach computers and devices in various ways, including spam⁹ (with malicious file attachments or embedded links), compromised¹⁰ or specially crafted malicious websites or web pages, and exploit kits, most notably Angler.¹¹

Behaviors and Routines

Ransomware behaviors have dramatically changed over the past two years. In 2015, a shift in target was observed—operators started targeting businesses instead of individuals.¹² This was made evident with a constant stream of reports of big companies succumbing to the threat.

Apart from just infecting computers and mobile devices, ransomware also infected shared¹³ and removable drives¹⁴ and servers.¹⁵ Some families have also taken to encrypting chosen file types like tax-related and database files, ensuring bigger profits for their operators.

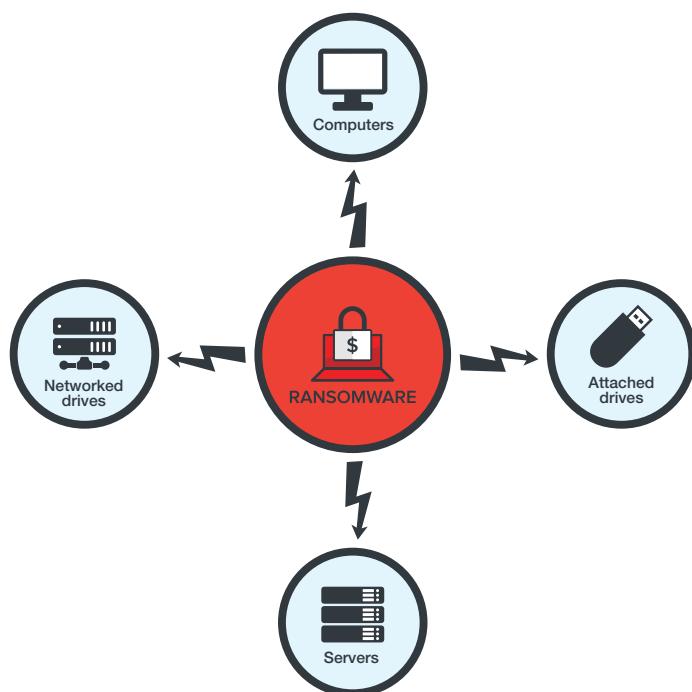


Figure 2. Devices that ransomware can infect

Ransom notes evolved as well. All forms of intimidation have been used, including the use of countdown timers until file deletion with increasing ransom amounts as more time elapses, and pop culture and current events references. Some variants like Doxware¹⁶ even threaten victims of data exposure if they do not pay up. This could be extra damaging to hospitals and healthcare providers who can get fined or litigated should they leak patient records.

Ease of Use

Ransomware's notoriety also led the most enterprising cybercrooks to make even more money. The ransomware-as-a-service (RaaS)¹⁷ business model made it possible for them to offer their malicious creations to others for a fee or a cut of the buyers' profits. Ransomware do-it-yourself (DIY) kits were also sold in underground markets and/or forums. And those who are short on budget can even frequent web repositories where open source ransomware like Hidden Tear¹⁸ can be had free of charge.

Ransom Demands

Besides MIRCOP,¹⁹ which demands a ludicrously high ransom, ransomware variants typically ask for 0.5–5 Bitcoins (as of 2016) in exchange for the victims' files. This is important for two reasons—some variants increase the ransom as more time elapses with nonpayment and the Bitcoin exchange rate is on the rise. In January 2016, 1 BTC was worth US\$431.²⁰ This has since almost tripled to US\$1,076.44 to date (exchange rate as of 21 March 2017).²¹

Though Bitcoins are the preferred mode of ransom payment, some ransomware like TrueCrypter²² use alternatives like Amazon gift cards.

2016: The Year Ransomware Reigned

Compared with the 29 ransomware families discovered in 2015, 2016 saw this number rise 752% to reach 247 in 2016.²³ And those behind the threat reportedly raked in US\$1 billion,²⁴ most likely a result of targeting large enterprises and organizations that did not have data backups and so resorted to paying the ransom.

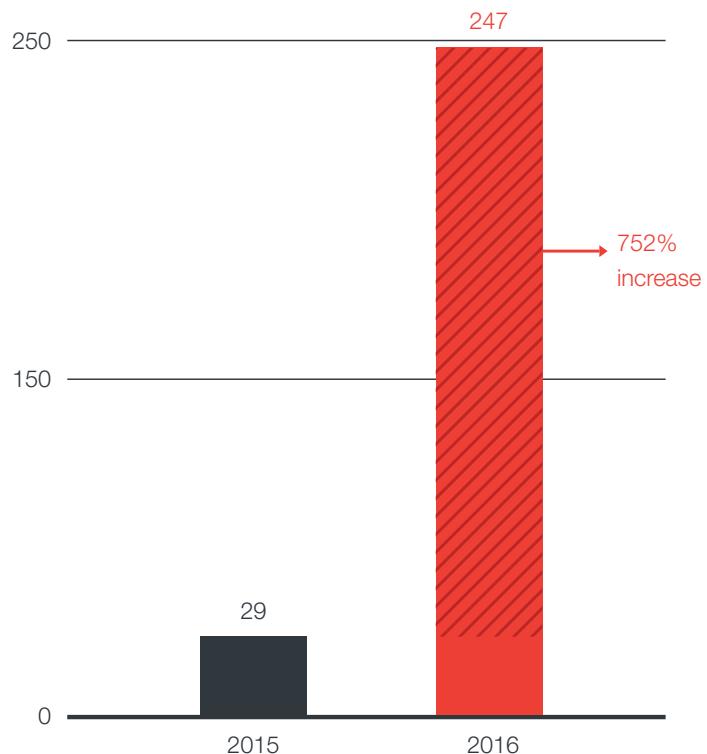


Figure 3. Number of newly added ransomware families, 2016

As usual, 79% of the ransomware Trend Micro detected and blocked arrived via spam. As best practice, potential victims are urged to keep in mind the level of social engineering used in spam campaigns. Popular events like holidays, sporting events, political news, and matters of interest or in a company's case, relevant business-related lures like the deadline for filing taxes can be used to get targets to download ransomware onto their systems. Infections that began with accessing ransomware-laden websites or web pages, meanwhile, accounted for 20% of the total.

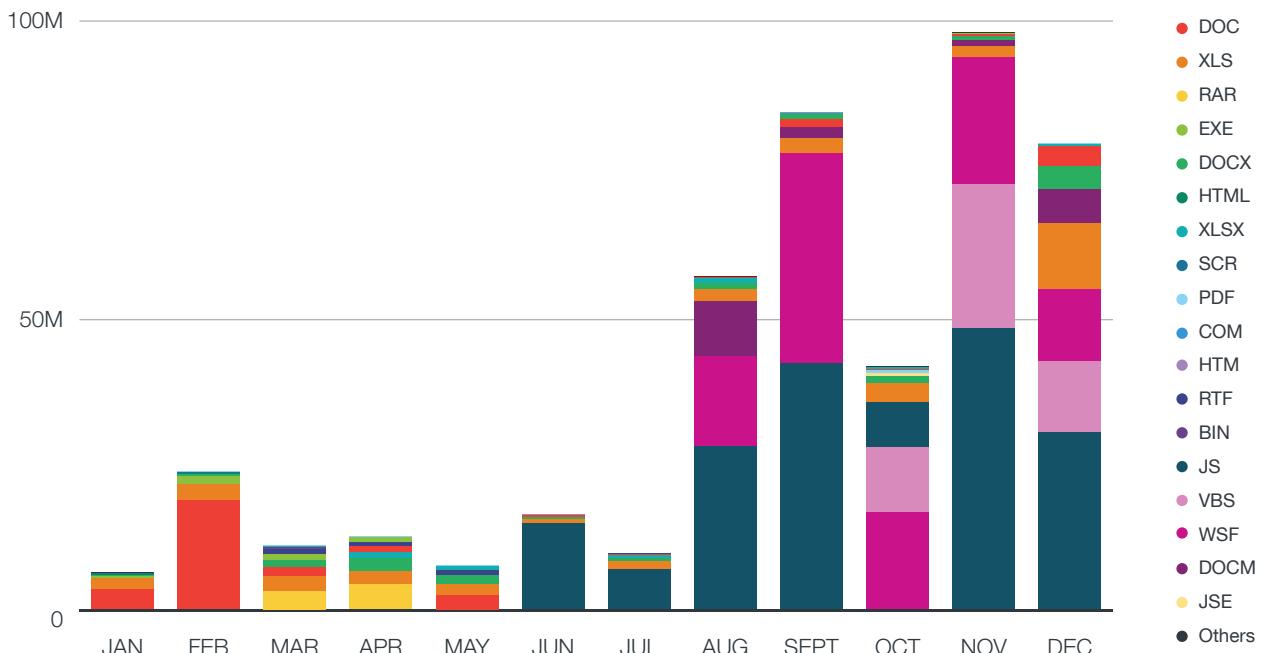


Figure 4. Top file types attached to ransomware-related spam, 2016

NOTE: The significant surge in JavaScript (JS) attachments in November was caused by NEMUCOD, a known ransomware dropper. LOCKY ransomware, which were distributed via email also contributed to this surge.

Ransomware operators that target enterprises encrypt business-critical files like databases in order to inflict the greatest amount of damage.

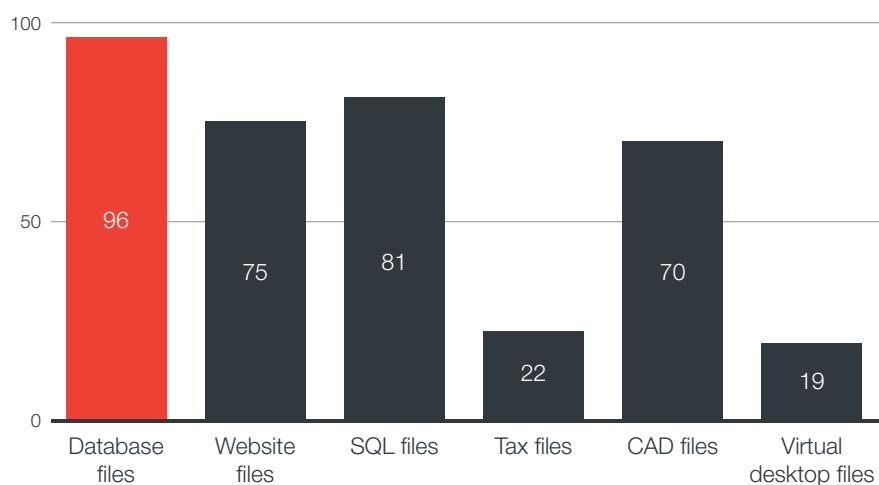
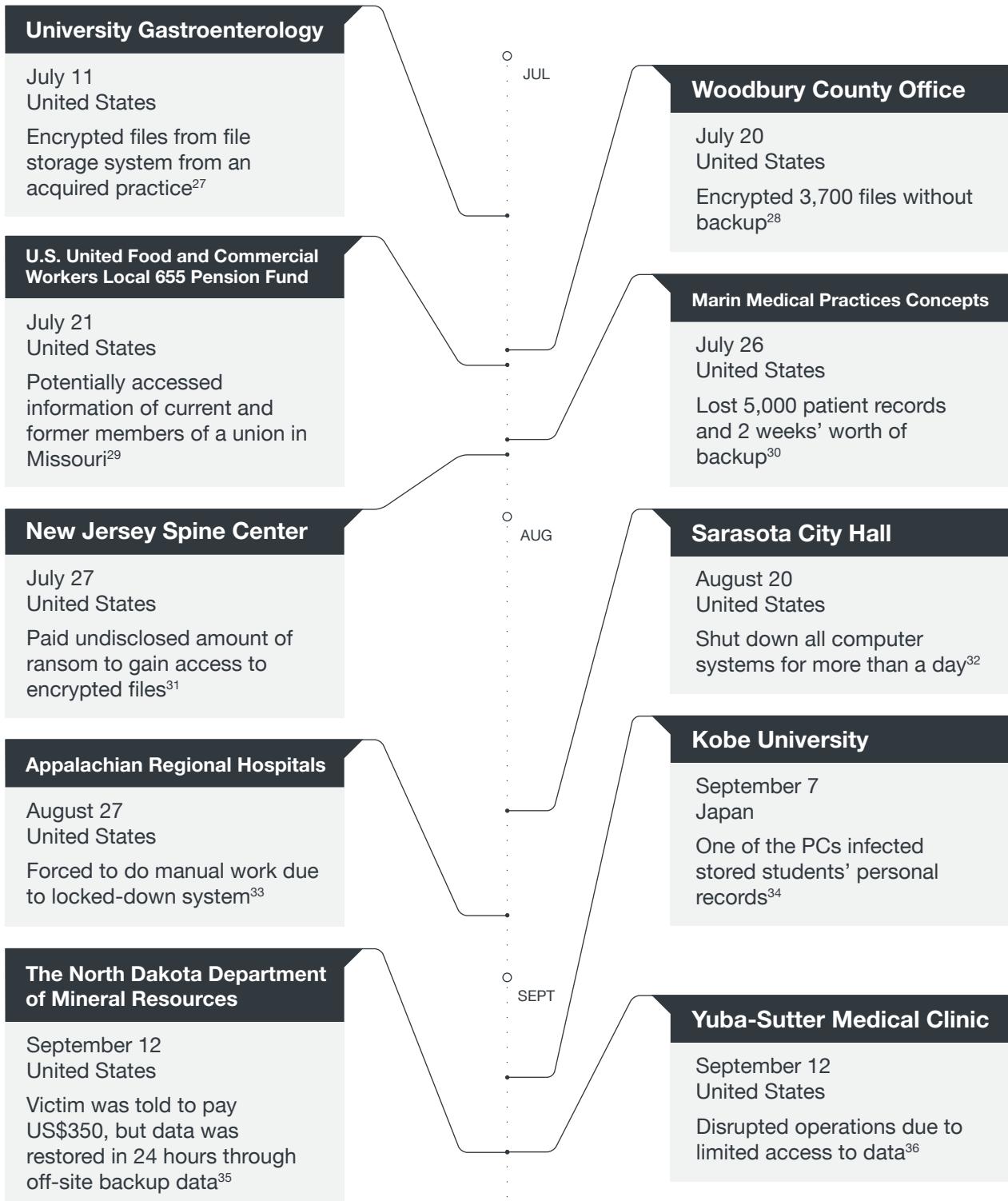
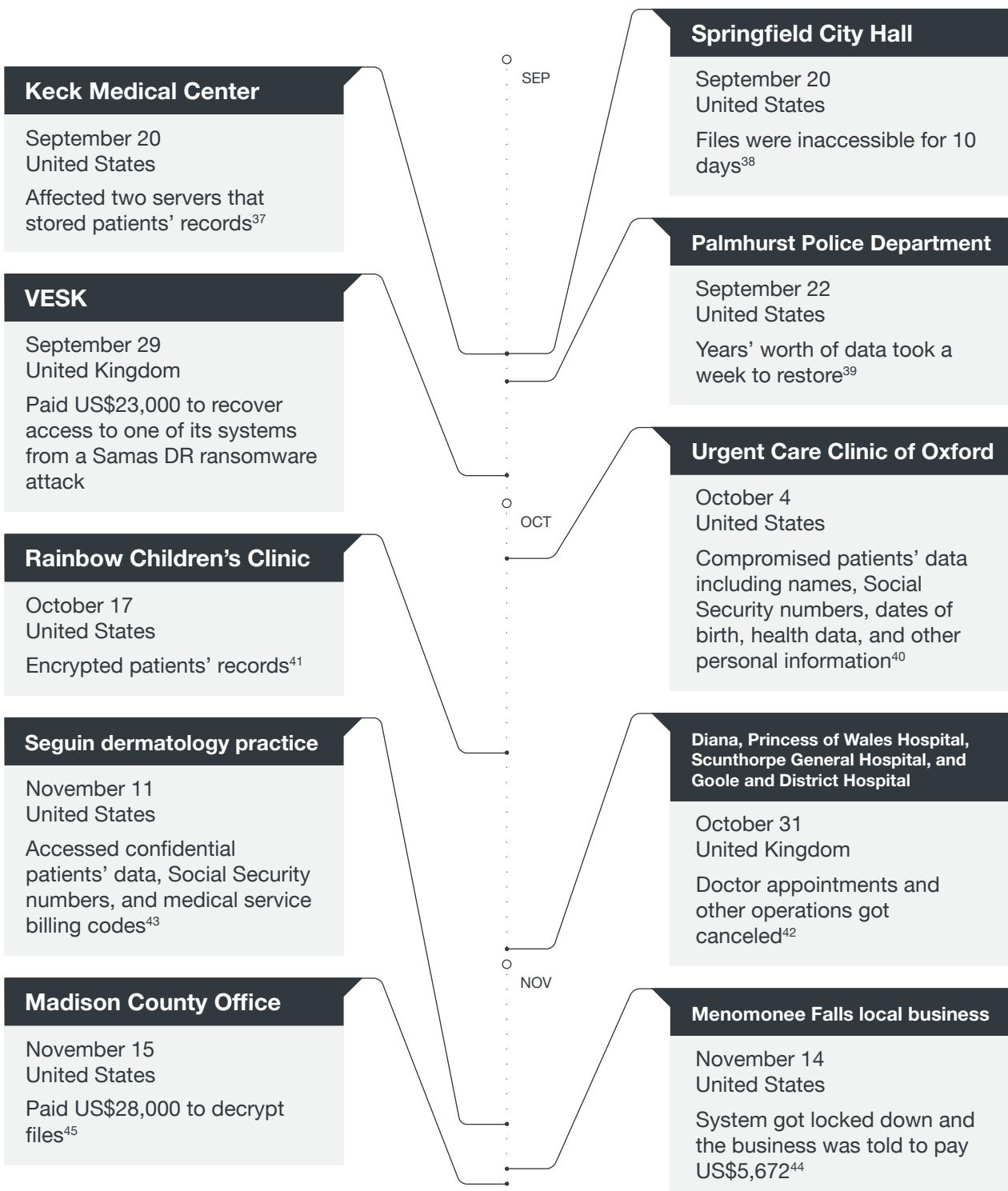


Figure 5. Number of known ransomware families that encrypt business-related files, 2016

Large enterprises and organizations, as previously mentioned, increasingly fell prey to ransomware over the years. We have seen educational institutions,²⁵ government offices, hospitals and healthcare service providers,²⁶ and other businesses succumb to attacks.





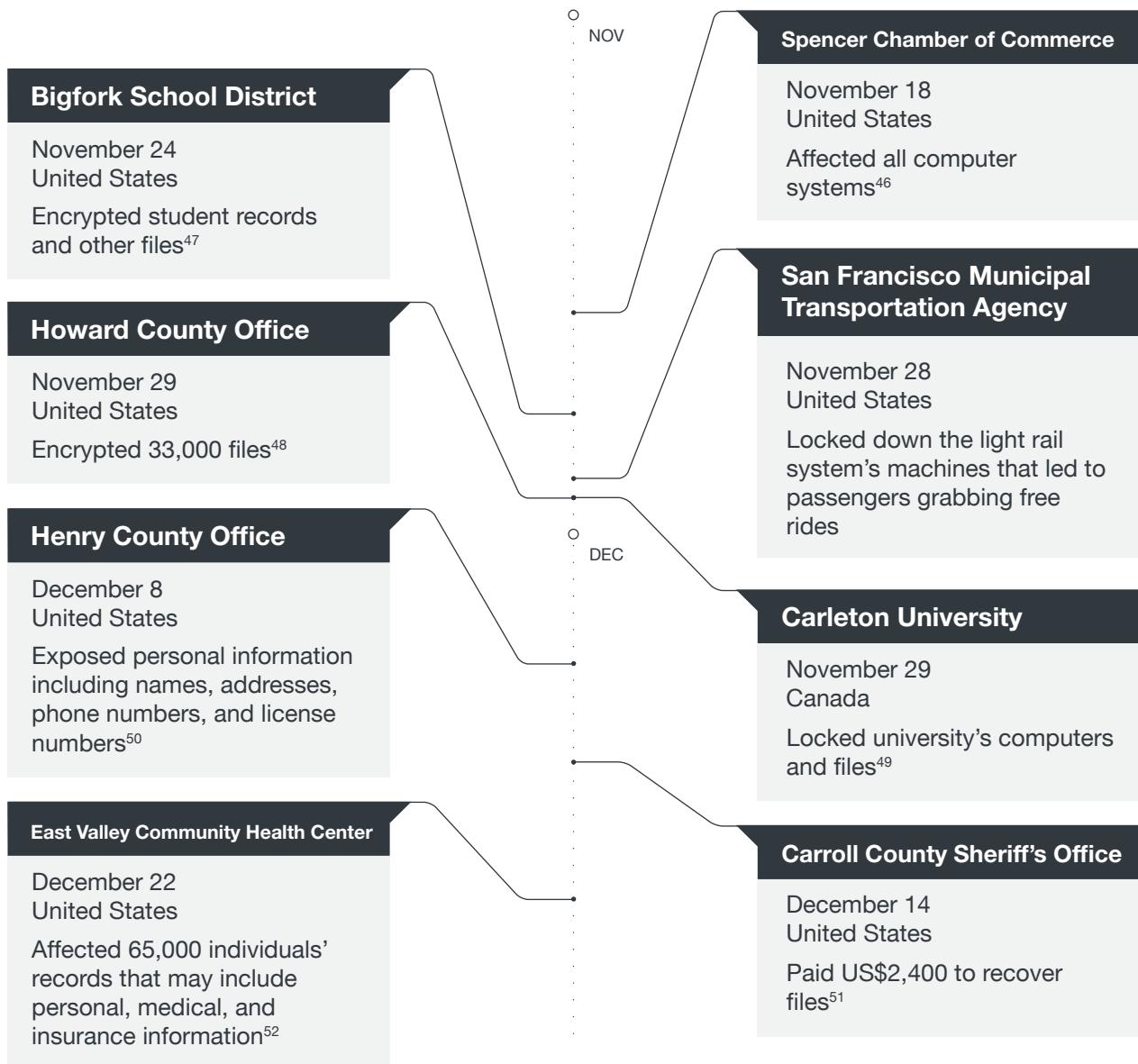


Figure 6. Ransomware incidents made public, 2H 2016

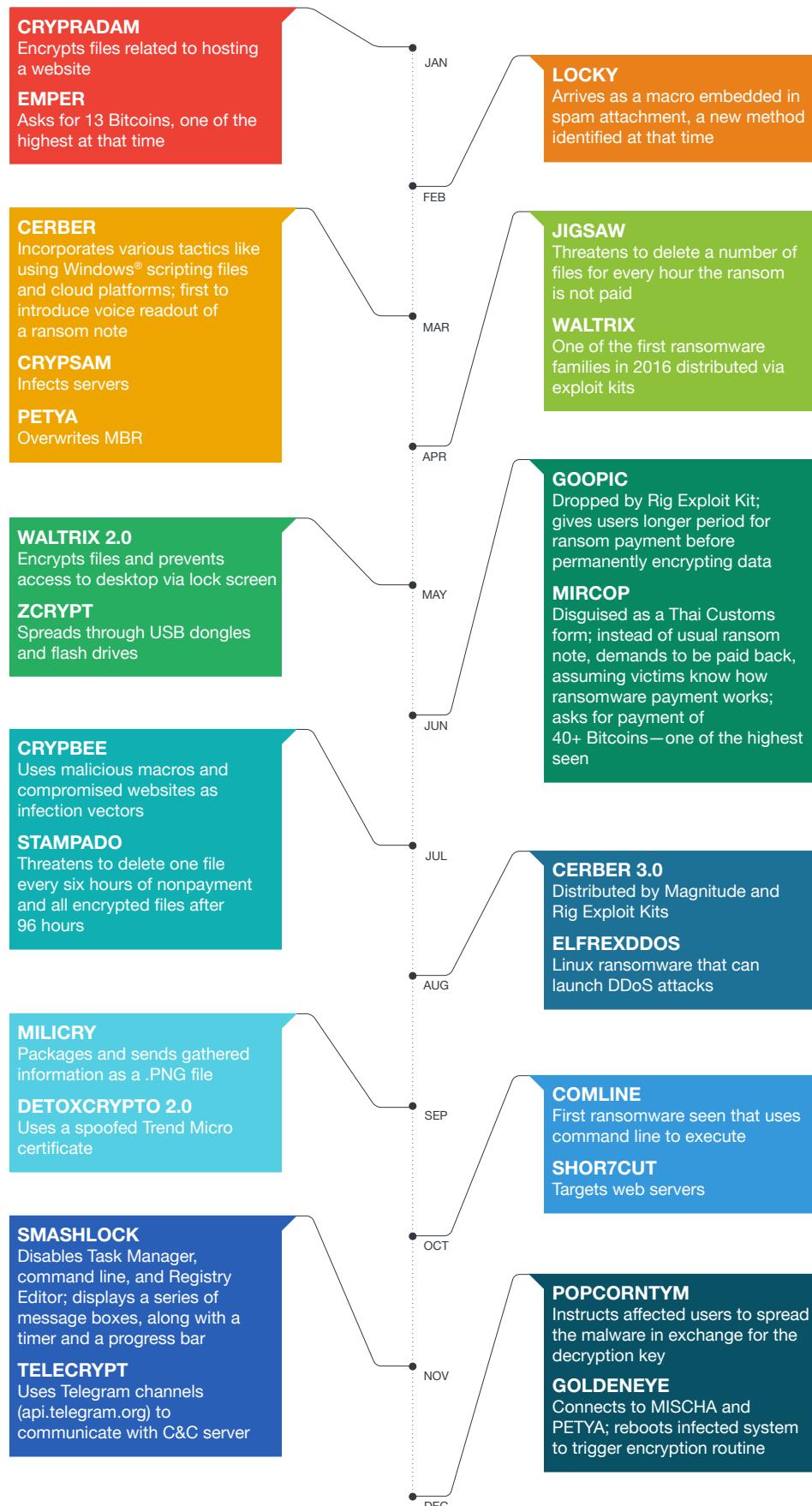


Figure 7. Timeline of noteworthy ransomware families, 2016

Latest Developments

Getting past security solutions installed on computers and other devices has always been a challenge for ransomware. A few families, in fact, introduced new ways for the threat to evade detection. The latest of this would be TorrentLocker, which started embedding compromised Dropbox URLs in phishing emails apart from using Nullsoft Scriptable Install System (NSIS) for encryption to get past installed security software.⁵³ The said URL leads to the download of a ransomware variant disguised as an invoice or some such document meant for the victim hosted on a legitimate site (and so access to it is not blocked), Dropbox.

In an effort to diversify targets, ransomware took another stab at Mac OS X® users with Patcher.⁵⁴ Apart from posing as a patcher for popular applications like Microsoft® Office® and Adobe® Premiere® Pro, Patcher also arrives via BitTorrent.

Hermes, another new ransomware variant, scans a victim's computer and unmapped network shares for files to encrypt then deletes System Restore points and reduces the allotted maximum shadow storage size to 410MB.⁵⁵

Though these routines are not altogether new, they still work and so are still used by ransomware. Case in point: ransomware variant WannaCry/WCRY, which originally spread via malicious Dropbox URLs embedded in spam, took an unexpected turn this May. It began exploiting a recently patched vulnerability in the SMB Server, thus resulting in the biggest ransomware attack to date.

Future Attacks

It will not be surprising if ransomware change in a few years. In terms of potential, they can evolve into malware that disable entire infrastructure (critical not only to a business's operation but also a city's or even a nation's) until the ransom is paid. Cybercriminals may soon look into approaches like hitting industrial control systems (ICS) and other critical infrastructure to paralyze not just networks but ecosystems. A key area that could become a bigger target for cybercriminals are payment systems, as seen with the Bay Area Transit attack in 2016 where the service provider's payment kiosks were targeted with ransomware.

We have seen ransomware operators hit hospitals and transportation service providers. What would stop attackers from hitting even bigger targets like the industrial robots that are widely used in the manufacturing sector or the infrastructure that connect and run today's smart cities? Online extortion is bound to make its way from taking computers and servers hostage to any type of insufficiently protected connected device, including smart devices, or critical infrastructure. The return on investment (ROI) and ease with which cybercriminals can create, launch, and profit from this threat will ensure it continues in the future.

Ransomware: Mitigation and Prevention

We recommend organizations take some basic precautions to minimize their risk of this threat. Below are steps they can take.

 Back Up and Restore Automated: 3 copies, 2 formats, 1 air-gapped from network	 Control Access Limit access to business-critical data
 Patch Minimize vulnerability exploitation	 Don't Pay the Ransom Pay-offs encourage further attacks
 Educate employees on phishing Awareness, best practices, simulation testing	 Improve Security Posture Behavior monitoring, additional technologies

Ransomware remain a top cybersecurity threat to this day. To target large enterprises and organizations, ransomware employ new routines that put valuable and even critical data at great risk. Security solutions that incorporate a cross-generational technology approach that combines reputation-based analysis with other anti-ransomware capabilities like whitelisting and application control, behavioral analysis, network monitoring, vulnerability shielding, and high-fidelity machine learning can better protect companies while minimizing the impact on their computing resources.

Variants like TorrentLocker can evade gateway detection with the use of legitimate URLs that redirect to ransomware-hosting web pages. To address these, a layered approach at the gateway is needed. This includes messaging and web gateway security solutions that can detect ransomware and phishing emails (with weaponized attachments or embedded malicious URLs) as well as a sandbox technology for files and web pages.

Patcher and similar families, which can encrypt files even on non-Windows computers, can be thwarted with the aid of mobile security apps that analyze malicious mobile apps and Unix-based solutions that can scan for malicious URLs or files on non-Windows-based systems.

Servers and networks that can be affected by ransomware like WannaCry, meanwhile, can stay protected with security products designed for physical, virtual, or cloud-based servers that include technologies to detect malicious URLs or files associated with ransomware.

Prevent ransomware infection on any system before your business suffers with the help of the wide array of Trend Micro email and gateway, endpoint, network, and server protection suites.



Email and Gateway Protection

Trend Micro™ Cloud App Security, Deep Discovery™ Email Inspector, and InterScan™ Web Security address ransomware tied to common delivery methods such as email and web pages.

Capabilities:

- ✓ Spear-phishing protection
- ✓ Malware sandboxing
- ✓ IP/Web reputation checking
- ✓ Document exploit detection



Endpoint Protection

Trend Micro Smart Protection Suites detects and stops suspicious behavior and exploits associated with ransomware at the endpoint level.

Capabilities:

- ✓ High-fidelity machine learning
- ✓ Ransomware behavior monitoring
- ✓ Application control
- ✓ Vulnerability shielding
- ✓ Web security provision



Network Protection

Trend Micro Deep Discovery Inspector detects malicious traffic, communications, and other activities associated with attempts to inject ransomware into the network.

Capabilities:

- ✓ Network traffic scanning
- ✓ Malware sandboxing
- ✓ Lateral movement prevention



Server Protection

Trend Micro Deep Security™ detects and stops suspicious network activity and shields servers and applications from exploits.

Capabilities:

- ✓ Web server protection
- ✓ Vulnerability shielding

Appendix

JAN	CRYPJOKER	CRYPNISCA	CRYPRADAM	CRYPTRITU
	EMPER	LECTOOL	MEMEKAP	
FEB	CRYPDAP	CRYPGPCODE	CRYPHYDRA 1.0	CRYPZUQUIT
	LOCKY	MADLOCKER		
MAR	CERBER	CRYPAURA	KERANGER	MAKTUB
	MAKTUB	SURPRISE	PETYA	TESLA
APR	COVERTON	CRYPSALAM	CRYPSAM	CRYPTEAR 1.0
	CRYPTOHASU	CRYPTOHOST 1.0	CRYPTOSO	CRYPTVAULT
MAY	EMPER 2.0	JIGSAW	KIMCIL	WALTRIX
	XORBAT	ZIPPY		
JUN	AUTOLOCKY	BADBLOCK	BLOCCATO	BRLOCK
	BUCBI	CRRIPTODC	CRYPALPHA	CRYPCORE
JUL	CRYPDAP	CRYPLIKI	CRYPMAME	DEMOCRY
	ELFACRYPT	ENIGMA	LOCKSCAM	MISCHA
AUG	ROKKU	SHUJIN	SNSLOCK	TAKALOCKER
	WALTRIX 2.0	ZCRYPT		
SEP	APOCALYPSE	BART	CRYPAGA	CRYPCUTE
	CRYPEDA	CRYPHERBST	CYPHERKEY	CRYPKEYIV
OCT	CRYPMIC 1.0	CRYPSHOCKER	GOOPIC	JIGSAW 2.0
	JOKOZY	JSRAA	LOCKRVTN	MIRCOP
	SATANA	WALTRIX 3.0	WALTRIX 4.0	WHITELOCK
	XORIST	ZIRBAM		
	ALFA	CRYPBEE	CRYPMIC 2.0	FAKELOCK
	HOLYCRYPT	JAGER	JUSINOMEL	NOOBCRYPT
	POWERWARE 2.0	RUSHTEAR	SANCTEAR	STAMPADO 1.0
	TILDE	UYARITEAR	WALTRIX 5.0	ZIPTB
	ALMALOCK	ATILOCKTEAR	BAKSOCUTE	BANKTEAR
	BART 2.0	CERBER 2.0	CERBER 3.0	CRYPHYDRA 2.0
	CRYPMIC 3.0	CRYPTLOCK	CRYPTOHOST 2.0	CRYPZXAS
	DETOXCRYPTO 1.0	DOMINO	ELFREXDDOS	FANTOMCRYPT
	FSOCEDA	KAOTEAR	LERITH	POGOTEAR
	PURGE	REKTEDA	SCRNLOCKER	SERPICO
	SHARKRAAS	SHINOLOCK	TELANATEAR	VENUSLOCK
	WILDFIRE			
	ATOM	CRYPTEAR 2.0	CRYPTTRX	CRYPY
	CRYYSIS	CUCKTOX	DETOXCRYPTO 2.0	EDALOCK
	EREBUS	FENIX	HDDCRYPTOR	HIDDENTEARBLACKFEATHER
	HIDDENTEARDEVMARE	HORCRUX	JOKEMARS	KAWAIILOCKER
	MILICRY	NULLBYTE	PrincessLocker	RARVAULT
	STAMPADO 2.0	STOPI		
	ALCATRAZ	ANGRYDUCK	CERBER 4.0	CLICKMEG
	ComCircle	COMLINE	CRYPTBTN	CRYPTGO
	CryptoTrooper	EDA2Anubis	EDA2BLA	EDA2JanBleed
	EDA2MasterBuster	EDA2Notorious	ENCRYPTILE	ENIGMA
	ESMERALDA	EXOTIC	HADESLOCK	HiddenTearAPT
	HiddenTearNotorious	HiddenTearShadow	JACKPOT	KILLERLOCKER
	KOSTYA	LERITH 2.0	LOCK93	NUCLEAR
	SHOR7CUT	Sonido	TENSEC	VENIS
	WILCRYPT			

NOV	AIRACROP	CERBER 4.1.6	CERBER 5.0.0	CERBER 5.0.1
	CHIP	CITOXE	CRYPAYSAFE	CRYPHYDRA
	CRYPTSHED	CRYPTASN1	CryptoLuck	CRYPTON
	CRYPTOWIRE	CRYYSIS 2.0	DXXD	EDA2Runsome
	EXOSHELL	GREMIT	HappyLocker	HiddenTearCerber
	HiddenTearDecryptor	HiddenTearHappy	HiddenTearHCrypto	HiddenTearHolly
	HiddenTearFSociety	HOTDEM	ILOCKED	ISHTAR
	KARMA	LOMIX	MATRIX	PayDOS
	PCLOCK	PROTOBTC	PSHELL	Ransoc
	RARLOCK	RAZCRYPT	RUNELOCKER	SMASHLOCK
	SPICYCRYPT	SURVEYLOCK	TELECRYPT	VINDOWS
	ZEROCRYPT			
	ADAMLOCK	ANTIX	AYTEP	BADSCRIPT
	BRAINCRYPT	CERBER 5.0.x	CRYPBLOCK	CRYPEXTX
DEC	CRYPTORIUM	DERIALOCK	DESBLOQ	DONATO
	EDGELOCKER	FREROGA	GOLDENEYE	HiddenTearGuster
	HiddenTearKoko	LEVILOCK	MFESTUS	MICROP
	PopCornTym	SCRLOCKER		

Table 1. Ransomware families seen in 2016

	Database	Website	SQL	Tax	CAD	VD
ALFA	•		•		•	
Antix	•	•	•		•	•
ATILOCKTEAR		•	•			
AUTOLOCKY	•	•			•	
BADBLOCK	•	•	•		•	
BAKSOCUTE		•			•	
BART	•	•	•			•
CERBER	•		•		•	
CITOXE	•	•	•		•	
CRPTODC	•		•	•	•	
CRYPALPHA	•	•	•		•	
CRYPAURA	•	•	•		•	
CRYPBEE				•	•	•
CRYPCORE	•				•	
CRYPCUTE	•	•	•		•	
CRYPDAP	•	•	•		•	

	Database	Website	SQL	Tax	CAD	VD
CRYPEDA		•				
CRYPGPCODE	•	•	•	•	•	
CRYPHYDRA	•	•	•	•	•	
CRYPJOKER	•	•	•		•	
CRYPKEYIV	•	•	•			
CRYPLIKI	•		•	•	•	
CRYPLIKI	•	•	•	•		
CRYPMIC 1.0	•	•	•		•	•
CRYPMIC 2.0	•		•		•	
CRYPNISCA	•	•	•			
CRYPRADAM	•	•	•	•	•	
CRYPSHED		•				
CRYPSHOCKER	•		•	•	•	
CRYPTEAR 1.0	•	•			•	
CRYPTOHOST 1.0	•	•			•	•
CryptoLuck	•	•	•		•	
CRYPTBTN	•					
CRYPTON	•					
CRYPTOSO	•	•	•		•	
CRYPTRITU	•	•	•		•	
CRYPVULT		•				
CRYYSIS 2.0	•			•	•	
DETOXCRYPTO 2.0	•		•			
DXXD	•		•			•
EDA2BLA	•	•	•			
EDA2JanBleed	•		•			
EDA2Runsome	•	•	•		•	
ELFACRYPT	•				•	
EMPER	•		•		•	

	Database	Website	SQL	Tax	CAD	VD
EMPER 2.0			•		•	
ENIGMA	•	•	•		•	•
EREBUS	•	•	•	•		•
GOLDENEYE	•	•	•		•	
HADESLOCK	•		•		•	•
HiddenTearAPT	•	•	•		•	
HiddenTearCerber	•	•	•		•	
HiddenTearDecryptor	•	•	•			
HiddenTearFSociety	•	•	•		•	
HiddenTearGuster	•	•	•			
HiddenTearHappy	•	•	•		•	
HiddenTearHolly	•	•				
HiddenTearKoko	•	•	•		•	
HiddenTearShadow	•	•	•			
HOLYCRYPT	•	•	•			
HOTDEM	•	•	•	•	•	
ISHTAR	•			•		
JIGSAW	•	•	•		•	•
JIGSAW 2.0	•	•	•		•	
JOKEMARS	•	•	•	•	•	
JOKOZY	•					
JSRAA	•				•	
KERANGER	•		•	•	•	
KIMCIL	•	•	•			
KOSTYA	•					
LECTOOL	•		•			
LOCK93	•	•				
LOCKY	•		•			
MADLOCKER	•	•	•			•

	Database	Website	SQL	Tax	CAD	VD
MAKTUB	•	•	•	•	•	
MIRCOP	•	•	•			
MISCHA	•	•	•		•	
PCLOCK	•				•	
PETYA	•	•	•	•	•	
POGOTEAR		•	•			
PopCornTym	•	•	•	•	•	•
POWERWARE 2.0				•	•	
PrincessLocker	•		•		•	
PROTOBTC	•			•	•	
PSHELL						
REKTEDA		•	•			
ROKKU	•	•	•	•	•	
RUSHTEAR		•	•			
SATANA	•			•	•	
SEOIRSE	•	•	•			
SHOR7CUT		•				
SPICYCRYPT	•	•	•		•	
STAMPADO 1.0	•	•			•	
TAKALOCKER		•	•			
TESLA	•		•	•	•	
UYARITEAR	•				•	
VENUSLOCK		•				•
VINDOWS	•	•	•			
WALTRIX	•	•			•	•
WALTRIX 2.0	•	•	•		•	•
WALTRIX 3.0	•	•	•		•	•
WALTRIX 4.0	•	•	•		•	•
WALTRIX 5.0	•		•			•

	Database	Website	SQL	Tax	CAD	VD
XORBAT	•	•	•		•	
XORIST	•		•		•	
ZCRYPT	•	•	•		•	
ZEROCRYPT		•				
ZIPPY	•		•			

Table 2. Business-related files encrypted by known ransomware families in 2016

References

1. TrendLabs. (2017). *Threat Encyclopedia*. “Ransomware.” Last accessed on 20 March 2017, <https://www.trendmicro.com/vinfo/us/security/definition/Ransomware>.
2. Trend Micro Incorporated. (14 March 2006). *TrendLabs Security Intelligence Blog*. “Ransomware! Ransomware! Ransomware!” Last accessed on 20 March 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware21-ransomware21-ransomware21/>.
3. Nart Villeneuve. (12 January 2011). *TrendLabs Security Intelligence Blog*. “SMS Ransomware Tricks Russian Users.” Last accessed on 20 March 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/sms-ransomware-tricks-russian-users/>.
4. Cris Pantanilla. (12 April 2012). *TrendLabs Security Intelligence Blog*. “Ransomware Takes MBR Hostage.” Last accessed on 20 March 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-takes-mbr-hostage/>.
5. Roland Dela Paz. (8 March 2012). *TrendLabs Security Intelligence Blog*. “Ransomware Attacks Continue to Spread Across Europe.” Last accessed on 20 March 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-attacks-continue-to-spread-across-europe/>.
6. Oscar Celestino Angelo Abendan II. (22 March 2012). *Trend Micro Threat Encyclopedia*. “Dwindling FAKEAV Business Spurs Ransomware Infections in Europe.” Last accessed on 10 April 2017, <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/122/dwindling-fakeav-business-spurs-ransomware-infections-in-europe>.
7. David Sancho. (2012). *Trend Micro Security Intelligence*. “Police Ransomware Update.” Last accessed on 21 March 2017, <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-police-ransomware-update.pdf>.
8. Joselito Dela Cruz. (11 October 2013). *TrendLabs Security Intelligence Blog*. “Threat Refinement Ensues with CryptoLocker, SHOTODOR Backdoor.” Last accessed on 21 March 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/threat-refinement-ensues-with-crypto-locker-shotodor-backdoor>.
9. Kervin Alintanahin. (21 October 2013). *TrendLabs Security Intelligence Blog*. “CryptoLocker: Its Spam and ZeuS/ZBOT Connection.” Last accessed on 21 March 2017, [http://blog.trendmicro.com/trendlabs-security-intelligence/cryptolocker-its-spam-and-zeusbot-connection/](http://blog.trendmicro.com/trendlabs-security-intelligence/cryptolocker-its-spam-and-zeusbot-connection).
10. Robert McArdle. (22 February 2012). *TrendLabs Security Intelligence Blog*. “Compromised Website for Luxury Cakes and Pastries Spreads Ransomware.” Last accessed on 21 March 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/compromised-website-for-luxury-cakes-and-pastries-spreads-ransomware>.
11. Joseph C. Chen. (22 June 2016). *TrendLabs Security Intelligence Blog*. “After Angler: Shift in Exploit Kit Landscape and New Crypto-Ransomware Activity.” Last accessed on 21 March 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/angler-shift-ek-landscape-new-crypto-ransomware-activity>.
12. Paul Pajares. (22 September 2015). *TrendLabs Security Intelligence Blog*. “Businesses Held for Ransom: TorrentLocker and CryptoWall Change Tactics.” Last accessed on 21 March 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/businesses-held-for-ransom-torrentlocker-and-cryptowall-change-tactics>.
13. Trend Micro Incorporated. (7 August 2015). *TrendLabs Security Intelligence Blog*. “Price Hikes and Deadlines: Updates in the World of Ransomware.” Last accessed on 21 March 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/price-hikes-and-deadlines-updates-in-the-world-of-ransomware>.
14. Abigail Pichel. (25 December 2013). *TrendLabs Security Intelligence Blog*. “New CryptoLocker Spreads via Removable Drives.” Last accessed on 21 March 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/new-cryptolocker-spreads-via-removable-drives>.
15. Trend Micro Incorporated. (22 April 2016). *TrendLabs Security Intelligence Blog*. “A Lesson on Patching: The Rise of SAMSAM Crypto-Ransomware.” Last accessed on 21 March 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/lesson-patching-rise-samsam-crypto-ransomware>.

16. NETWORTH. (26 January 2017). *NETWORTH*. “Doxware Ransomware Threatens to Release Sensitive Info Publicly.” Last accessed on 10 April 2017, <http://www.networth.ca/2017/01/doxware-ransomware-threatens-release-sensitive-info-publicly/>.
17. TrendLabs. (7 September 2016). *Trend Micro Security News*. “Ransomware as a Service Offered in the Deep Web: What This Means for Enterprises.” Last accessed on 21 March 2017, <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-what-this-means-for-enterprises>.
18. Trend Micro Incorporated. (25 August 2016). *TrendLabs Security Intelligence Blog*. “New Open Source Ransomware Based on Hidden Tear and EDA2 May Target Businesses.” Last accessed on 21 March 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/new-open-source-ransomware-based-on-hidden-tear-and-eda2-may-target-businesses>.
19. Jaaziel Carlos. (24 June 2016). *TrendLabs Security Intelligence Blog*. “MIRCOP Crypto-Ransomware Channels Guy Fawkes, Claims to Be the Victim Instead.” Last accessed on 21 March 2017, [http://blog.trendmicro.com/trendlabs-security-intelligence/instruction-less-ransomware-mircop-channels-guy-fawkes/](http://blog.trendmicro.com/trendlabs-security-intelligence/instruction-less-ransomware-mircop-channels-guy-fawkes).
20. Pesa_Mic. (20 January 2016). *Deep.Dot.Web*. “Bitcoin Price Analysis 20-Jan-2016.” Last accessed on 21 March 2017, <https://www.deepdotweb.com/2016/01/20/bitcoin-price-analysis-20-jan-2016/>.
21. XE. (1995–2017). *XE*. “XBT—Bitcoin.” Last accessed on 21 March 2017, <http://www.xe.com/currency/xbt-bitcoin>.
22. TrendLabs. (2 May 2016). *Trend Micro Security News*. “TrueCrypter Ransomware Now Accepting Amazon Gift Cards.” Last accessed on 21 March 2017, <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/truecrypter-ransomware-accepting-amazon-gift-cards>.
23. TrendLabs. (28 February 2017). *Trend Micro Security News*. “A Record Year for Enterprise Threats.” Last accessed on 21 March 2017, <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup>.
24. Maria Korolov. (5 January 2017). *CSO*. “Ransomware Took in \$1 Billion in 2016—Improved Defenses May Not Be Enough to Stem the Tide.” Last accessed 21 March 2017, <http://www.csoonline.com/article/3154714/security/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html>.
25. TrendLabs. (9 September 2016). *Trend Micro Security News*. “Countering the Education Sector’s Ransomware Problem.” Last accessed on 21 March 2017, <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/countering-the-education-sector-s-ransomware-problem>.
26. TrendLabs. (31 March 2016). *Trend Micro Security News*. “Hospital Ransomware on the Loose? More Healthcare Providers Affected by Ransomware.” Last accessed on 31 March 2017, <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hospital-ransomware-on-the-loose-more-healthcare-providers-affected-by-ransomware>.
27. Kayla Thrailkill. (13 September 2016). *TechTalk*. “University Gastroenterology Informs Patients of Data Security Incident.” Last accessed on 21 March 2017, <http://techtalk.pcpitstop.com/2016/09/13/ugi-security-incident/>.
28. Ian Richardson. (2 August 2016). *Sioux City Journal*. “Supervisors Approve Investigation into Cyber Attack That Compromised 3,700 County Files.” Last accessed on 21 March 2017, http://siouxcityjournal.com/news/supervisors-approve-investigation-into-cyber-attack-that-compromised-county-files/article_6273cb18-7704-5803-bd66-c88a9931a4d0.html.
29. Kaitlyn Schwers. (16 November 2016). *Belleville News-Democrat*. “Unionized Grocery Workers May Be Victimized by Computer Hack.” Last accessed on 21 March 2107, <http://www.bnd.com/news/local/article115148918.html>.
30. Jessica Davis. (5 October 2016). *Healthcare IT News*. “Two Providers Forced to Pay Up in Ransomware Attacks.” Last accessed on 21 March 2017, <http://www.healthcareitnews.com/news/two-more-ransomware-attacks-both-organizations-pay>.
31. Akanksha Jayanthi. (4 October 2016). *Becker’s Health IT & CIO Review*. “New Jersey Spine Center Pays Ransom to Cyber Attackers After ‘Seeing No Other Option.’” Last accessed on 21 March 2017, <http://www.beckershospitalreview.com/healthcare-information-technology/new-jersey-spine-center-pays-ransom-to-cyberattackers-after-seeing-no-other-option.html>.
32. WWSB ABC 7. (20 August 2016). *WWSB ABC 7 My Suncoast*. “City of Sarasota’s System Hacked by Ransomware, Data Held Hostage.” Last accessed on 21 March 2017, http://www.mysuncoast.com/news/local/city-of-sarasota-s-system-hacked-by-ransomware-data-held/article_706019e2-6635-11e6-94cc-af3af2bb01f1.html.

33. Daniel Tyson. (27 August 2016). *The Register-Herald.com*. "ARH Computers Breached." Last accessed on 21 March 2017, http://www.register-herald.com/news/arh-computers-breached/article_5159665b-7786-523b-b233-c3524259b538.html.
34. Public Relations Division, General Affairs Department. (7 September 2016). *Kobe University*. "On the Computer Virus Infection of Our Professional Computer." Last accessed on 21 March 2017, http://www.kobe-u.ac.jp/NEWS/info/2016_09_07_01.html.
35. Amy Dalrymple. (12 September 2016). *Grand Forks Herald*. "ND Department Attacked by Ransomware." Last accessed on 21 March 2017, <http://www.grandforksherald.com/news/4113494-nd-department-attacked-ransomware>.
36. Monica Vaughan. (12 September 2016). *Prospect Magazine*. "Ransomware Attack Hits Yuba City Clinic." Last accessed on 21 March 2017, http://www.appeal-democrat.com/news/ransomware-attack-hits-yuba-city-clinic/article_23755354-7954-11e6-8506-5f7d1b5d1d53.html.
37. Rodney Hanners. (20 September 2016). *Keck Medical Center of USC*. "Notice of Data Breach." Last accessed on 21 March 2017, <http://www.keckmedicine.org/wp-content/uploads/2016/09/doc11167320160920094345.pdf>.
38. Nicole Young. (20 September 2016). *The Tennessean*. "Springfield City Hall Recovers from Ransomware Attack." Last accessed on 21 March 2017, <http://www.tennessean.com/story/news/local/robertson/2016/09/20/springfield-city-hall-recovers-ransomware-attack/90746176/>.
39. Frankly Media and krgv. (22 September 2016). *KRGV.com*. "Palmhurst Police Department Avoids Data Loss." Last accessed on 21 March 2017, <http://www.krgv.com/story/33153212/palmhurst-police-department-avoids-data-loss>.
40. Jessica Davis. (4 October 2016). *Healthcare IT News*. "Ransomware Attack on Urgent Care Clinic of Oxford, Purportedly Caused by Russian Hackers." Last accessed on 21 March 2017, <http://www.healthcareitnews.com/node/530046>.
41. Dissent. (17 October 2016). *Office of Inadequate Security*. "Rainbow Children's Clinic Notifies 33,368 Patients of Ransomware Attack." Last accessed on 21 March 2017, <https://www.databreaches.net/rainbow-childrens-clinic-notifies-33368-patients-of-ransomware-attack/>.
42. Abe Hawken. (31 October 2016). *MailOnline*. "NHS Trust Cancels Every Operation at Three Hospitals After Its Electronic System Was Hit by a Computer Virus Attack." Last accessed on 21 March 2017, <http://www.dailymail.co.uk/news/article-3890964/NHS-Trust-cancels-operation-three-hospitals-electronic-hit-computer-virus-attack.html>.
43. Lynn Brezosky. (11 November 2016). *San Antonio Express News*. "Ransomware Attack Targets Seguin Dermatology Practice." Last accessed on 21 March 2017, <http://www.expressnews.com/business/local/article/Ransomware-attack-targets-Seguin-dermatology-10609268.php>.
44. Brittany Seemuth. (10 November 2016). *Northwest Now*. "Cyber Ransomming Hits Menomonee Falls Businesses." Last accessed on 21 March 2017, <http://www.mynorthwestnow.com/story/news/local/menomonee-falls/2016/11/10/cyber-ransomming-hits-menomonee-falls-businesses/93548816/>.
45. Herald Bulletin. (15 November 2016). *Indiana Economic Digest*. "Editorial: Madison County Hacker Attack Will Cost More Than Ransom Payment." Last accessed on 21 March 2017, <http://indianaeconomicdigest.com/main.asp?SectionID=31&subsectionID=201&articleID=85949>.
46. Kayla Threlkill. (18 November 2016). *TechTalk*. "Spencer Chamber of Commerce Infected with Ransomware." Last accessed on 21 March 2017, <http://techtalk.pcpitstop.com/2016/11/18/spencer-chamber-infected-ransomware/>.
47. Associated Press. (24 November 2016). *Billings Gazette*. "Ransomware Attack on Bigfork Schools; Fix in Works." Last accessed on 21 March 2017, http://billingsgazette.com/news/state-and-regional/montana/ransomware-attack-on-bigfork-schools-fix-in-works/article_7ff38855-e5a1-59d8-84de-18869e1c0df6.html.
48. Devin Zimmerman. (29 November 2016). *Kokomo Perspective*. "Ransomware Targets Howard County Government." Last accessed on 21 March 2017, http://kokomoperspective.com/kp/news/ransomware-targets-howard-county-government/article_9a6d8640-b5bb-11e6-854b-ff832671083f.html.
49. Matthew Braga. (29 November 2016). *CBCNews*. "Carleton University Computers Infected with Ransomware." Last accessed on 21 March 2017, <http://www.cbc.ca/news/technology/ransomware-carleton-university-computers-bitcoin-infects-1.3872702>.

50. Erin Allen. (8 December 2016). *TechTalk*. "Henry County Hit with Ransomware, Leaving 18,000 Voters as Victims." Last accessed on 21 March 2017, <http://techtalk.pcpitstop.com/2016/12/08/henry-county-hit-ransomware-leaving-18000-voters-victims/>.
51. Erin Allen. (14 December 2016). *TechTalk*. "Ransomware Strikes Arkansas Sheriff's Office." Last accessed on 21 March 2017, <http://techtalk.pcpitstop.com/2016/12/14/ransomware-strikes-arkansas-sheriffs-office/>.
52. Joseph Goedert. (22 December 2016). *Information Management*. "California Health Center Ransomware Attack Affects 65,000." Last accessed on 21 March 2017, <https://www.information-management.com/news/california-health-center-ransomware-attack-affects-65-000>.
53. Jon Oliver. (9 March 2017). *TrendLabs Security Intelligence Blog*. "TorrentLocker Changes Attack Method, Targets Leading European Countries." Last accessed on 21 March 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/torrentlocker-changes-attack-method-targets-leading-european-countries/>.
54. TrendLabs. (2 March 2017). *Trend Micro Security News*. "Ransomware Recap: Patcher Ransomware Targets Mac OS." Last accessed on 21 March 2017, <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-patcher-ransomware-targets-macos>.
55. Trend Micro Incorporated. (22 February 2017). *Trend Micro Threat Encyclopedia*. "RANSOM_HERMES.A." Last accessed on 21 March 2017, https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/ransom_hermes.a.



Created by:

TrendLabs

The Global Technical Support & R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com



Securing Your Journey
to the Cloud