THREAT INTEL REPORT

History of Ransomware

What is ransomware?

Ransomware is a type of malicious software, or malware, that denies a victim access to a computer system or data until a ransom is paid.[1] The first case of ransomware occurred in 1989 and has since evolved into one of the most profitable cybercrimes. This evolution is charted in Figure 1 at the end of the report, for easy visual reference of the timeline discussed below.

1989: The AIDS Trojan

The first ransomware virus was created by Harvard-trained evolutionary biologist Joseph L. Popp in 1989.[2] Popp conducted the attack by distributing 20,000 floppy discs to AIDS researchers from 90 countries that attended the World Health Organizations (WHO) International AIDS Conference in Stockholm.[3] Popp claimed that the discs contained a program that analyzed an individual's risk of acquiring AIDS through a risk questionnaire.[4] However, the disc contained a malware program that hid file directories, locked file names, and demanded victims send $189 to a P.O. box in Panama if the victims wanted their data back.[5] Referred to as the "AIDS Trojan" and the "PS Cyborg," the malware utilized simple symmetric cryptography and tools were soon available to decrypt the file names.[6] The healthcare industry remains a popular target of ransomware attacks over thirty years after the AIDS Trojan.

2005: GPCoder and Archiveus

The next evolution of ransomware emerged after computing was transformed by the internet in the early 2000s. One of the first examples of ransomware distributed online was the GPCoder

---

[1] "Ransomware," Cybersecurity and Infrastructure Security Agency, 2020, **https://www.us-cert.gov/Ransomware.**

[2] "Ransomware," KnowBe4, 2020, **https://www.knowbe4.com/ransomware**.

[3] "Ransomware," KnowBe4.

[4] Juliana De Groot, "A History of Ransomware," *Digital Guardian,* October 24, 2019, **https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time**.

[5] Ibid.

[6] Ibid.

Trojan.[7] GPCoder was first discovered in 2005 and infected Windows systems and targeted files with a variety of extensions.[8] Discovered files were copied in encrypted form and then original files were deleted.[9] The new encrypted files were unreadable, and the use of strong RSA-1024 encryption thwarted any attempts to unlock them.[10] A message was displayed on the victim's home screen with information on how to pay the ransom and unlock the files.

A second trojan utilizing secure RSA-1024 encryption known as Archiveus also emerged in 2005. Archiveus encrypted everything in the victim's documents folder instead of targeting specific executable files and files extensions.[11] Victims could still use their computers, but experienced restrictions in accessing most of their data. Victims were directed to a website to purchase a 30-digit password to recover their files.[12]

2008: The Invention of Bitcoin

Bitcoin is a decentralized cryptocurrency that first surfaced online in August 2008.[13] Bitcoin empowers cyber criminals to make ransom demands of digital currency, removing the inclusion of a transaction form for traditional currency.[14] Cyber criminals use bitcoin because it is "fast, reliable, and verifiable."[15] The attacker can watch the public blockchain to determine if a victim paid, and even make a unique payment address for each victim and automate the process of unlocking the victim's files upon payment.[16] Bitcoin became widely used in ransomware attacks in 2009.[17]

---

[7] "A History of the Ransomware Threat: Past, Present, and Future," *vpn Mentor,* 2020, **https://www.vpnmentor.com/blog/history-ransomware-threat-past-present-and-future/.**

[8] "A History of the Ransomware Threat: Past, Present, and Future," *vpn Mentor.*

[9] Ibid.

[10] Ibid.

[11] Ibid.

[12] Ibid.

[13] Zoe Bernard, "Everything you need to know about Bitcoin, its mysterious origins, and the many alleged identities of its creator," *Business Insider,* November 2018, **https://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12**.

[14] Tom Ball, "The History of Ransomware," *Computer Business Review,* February 2018, **https://www.cbronline.com/news/the-history-of-ransomware**.

[15] Neeraj Agrawal, "Why ransomware criminals use Bitcoin and why that could be undoing," Coin Center, May 2017, **https://coincenter.org/link/why-ransomware-criminals-use-bitcoin-and-why-that-could-be-their-undoing.**

[16] Neeraj Agrawal, "Why ransomware criminals use Bitcoin and why that could be undoing."

[17] Ball, "The History of Ransomware."

2009: Vundo, The Turning Point

Early forms of Trojan ransomware like GPCoder and Archievus generated low financial returns as they were easily detected and removed by anti-malware software.[18] Therefore, cyber criminals and gangs preferred to launch attacks via phishing and hacking to deceive victims with fictitious anti-viral scams prior to 2009.[19]

A known 'scareware' virus entitled Vundo evolved tactics and began to function as ransomware in 2009. Vundo previously infected computer systems and triggered its own fake security alert, prompting victims to a false fix.[20] However, attackers transformed Vundo into ransomware by using it to encrypt files on victim's computers, and then selling them a legitimate remedy to unlock the files in 2009.[21] This strategic shift in the execution of Vundo represented the first indication that attackers believed ransomware had the potential to become a profitable enterprise.[22] The proliferation of anonymous online payment platforms enabled attackers to receive ransom payments on a mass scale.[23] Furthermore, the increasing sophistication of ransomware methodology fueled its growth causing a ransomware boom between 2009 and 2011.

2011: Trojan Winlock

The WinLock Trojan appeared in 2011 and is considered the first widespread example of "Locker" ransomware. The locker prevents the ransomware victim from logging into their device and entire system instead of only encrypting the files.[24] The WinLock Trojan targeted Windows operating systems and copied the product activation system, keeping victims locked out until they purchased an activation key.[25] The WinLock Trojan prompted users to call a 'toll free' number that ended up racking up a significant bill to the attackers after the call ended.[26]

---

[18] "A History of the Ransomware Threat: Past, Present, and Future," *vpn Mentor.*

[19] Ibid.

[20] Ibid.

[21] Ibid.

[22] Ibid.

[23] Ibid.

[24] Ibid.

[25] "The Evolution of Ransomware: 2019 Brings the 30 Year Anniversary," Kraft, 2019, **https://kraftbusiness.com/cyber-security/evolution-of-ransomware-2019-brings-30-year-anniversary/**.

[26] "The Evolution of Ransomware: 2019 Brings the 30 Year Anniversary," Kraft.

2012: ‘Police’ Ransomware

The trend of imitating software to trick victims into paying with fake subscriptions evolved with the development of ‘police’ ransomware. Attackers would deploy malware that would target infected systems with messages claiming to represent law enforcement agencies.[27] Attackers informed victims that evidence related to criminal activity was discovered on the device and that it would remain locked until a fine was paid.[28] Police ransomware was often customized to make attacks seem more authentic by displaying the victim’s IP address, or a live feed from their own camera.[29]

2013-2015: Stronger Encryption

CryptoLocker surfaced in 2013 as a more aggressive and direct version of ransomware. CryptoLocker presented victims with two options: pay the ransom within three days, or all the files would be deleted.

CryptoLocker represented the advancements cyber criminals reached in encryption. CryptoLocker programmers used C2 servers on the hidden Tor network and produced 2048-bit RSA public and private key encryptions to infect files with specified extensions.[30] This acted as a dual protective measure: individuals would be unable to search for the public key as a base to decrypt the files as it was hidden on the Tor network, while the private key held by the programmers was independently strong.[31]

CryptoLocker also innovated a new distribution method. Infection initially spread via the Gameover Zeus botnet; a network of infected ‘zombie’ computers tasked with spreading malware throughout the internet.[32] Therefore, CryptoLocker signified the first ransomware spread through the medium of infected websites.[33] Successive ransomware adopted these CryptoLocker principles to replicate CryptoLocker’s lucrative success. The United States Department of Justice seized the Gameover Zeus botnet in 2014, therefore dismantling CryptoLocker.[34]

---

[27] Ibid.
[28] “A History of the Ransomware Threat: Past, Present, and Future,” *vpn Mentor.*
[29] Ibid.
[30] Ibid.
[31] Ibid.
[32] Ibid.
[33] Ibid.
[34] Mark Anthony Fuentes, ”A Brief History of Ransomware,” Horangi Cybersecurity, September 2019, **https://www.horangi.com/blog/a-brief-history-of-ransomware**.

2016: Locky and KeRanger

Locky is one of the most dangerous examples of ransomware due to the expediency and scale it infected computers.[35] Locky distributed via phishing attacks with malicious Microsoft Word attachments and infected up to 100,000 new systems every day at its peak performance.[36] Locky also changed encrypted file names making it very difficult to correctly restore data.[37]

KeRanger emerged as the first ransomware that targeted Mac computer systems. KeRanger targeted Mac files and the Mac's restore system, preventing the victim from restoring the system to a previous version.[38]

2017: Global Campaigns: WannaCry and Petya

Wannacry and Petya represent the first ransomware attacks that occurred on a widespread global scale.

Wannacry is a cryptoworm that semi-autonomously replicates and spreads automatically.[39] Wannacry marked a new phase in ransomware as it was the first ransomware that spread via targeted vulnerabilities on computers.[40]

Wannacry attacked its first victims in Spain in May 2016.[41] Within days, Wannacry infected a quarter of a million computers, representing the largest ransomware attack in history.[42]

Petya was another cryptoworm that exploited the same Windows vulnerabilities as Wannacry, despite the targeted release of security patches to remedy the issue.[43] Petya's success illustrates the urgency and necessity for patches in computer systems and environments.

2018: Grandcrab

Gandcrab is a Ransomware as a Service (RaaS) which allows any cybercriminal to utilize the software to execute attacks.[44] GandCrab is spread via malicious emails where the victim is

---

[35] "The Evolution of Ransomware: 2019 Brings the 30 Year Anniversary," Kraft.
[36] Ibid.
[37] "Locky Ransomware," KnowBe4, 2016, **https://www.knowbe4.com/locky-ransomware**.
[38] "The Evolution of Ransomware: 2019 Brings the 30 Year Anniversary," Kraft.
[39] "A History of the Ransomware Threat: Past, Present, and Future," *vpn Mentor.*
[40] Ibid.
[41] Ibid.
[42] Ibid.
[43] "The Evolution of Ransomware: 2019 Brings the 30 Year Anniversary," Kraft.
[44] Ibid.

prompted to download a zip file containing the ransomware.[45] The cybercriminals behind GandCrab announced they suspended operations in May 2019.[46]

2019: REvil and Sodinokibi

REvil ransomware, also known as Sodinokibi, was first discovered in Italy in May 2019 and is known as the successor of GandCrab.[47] REVil is a RaaS model for distribution and employs anti-kill technology to avoid detection by anti-malware software.[48] Sodinokibi spreads through Oracle WebLogic vulnerabilities, Flash UAF vulnerabilities, phishing emails, and RDP ports.[49]

2020: Ransomware Forecast

The Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) issued a 'high-impact' warning to U.S. businesses and organizations of ransomware in October 2019. The warning stated that indiscriminate ransomware campaigns sharply declined while 'losses from ransomware increased significantly as attacks become "more targeted, sophisticated and costly."'[50] Kivu assesses that ransomware attacks will reflect this trend in 2020.

Furthermore, we anticipate a surge in Ryuk ransomware attacks after the panic of the pandemic subsides. We assess it is highly likely that there will be an increase in ransomware attackers publicly releasing their victim's private and sensitive information to apply pressure on the victim to pay the ransom. We anticipate industries including healthcare, manufacturing, government organizations, education entities, and professional services will continue to remain the most targeted for ransomware attacks. We assess that spam and phishing emails will remain the most common attack vector for ransomware attacks and that phishing campaigns will continue to increase while much of the world's workforce continues to work from home.

---

[45] Ibid.

[46] "GandCrab," Malwarebytes, 2020, **https://www.malwarebytes.com/gandcrab/**.

[47] "The 10 Most Popular Types of Ransomware in 2019," Infotech News, January 2020, **https://meterpreter.org/the-10-most-popular-ransomware-in-2019/**.

[48] "The 10 Most Popular Types of Ransomware in 2019," Infotech News.

[49] Ibid.

[50] Davey Winder, "FBI Issues 'High-Impact' Cyber Attack Warning—What You Need to Know," *Forbes,* October 2019, **https://www.forbes.com/sites/daveywinder/2019/10/03/fbi-issues-high-impact-cyber-attack-warningwhat-you-need-to-know/#63af0e6740af**.

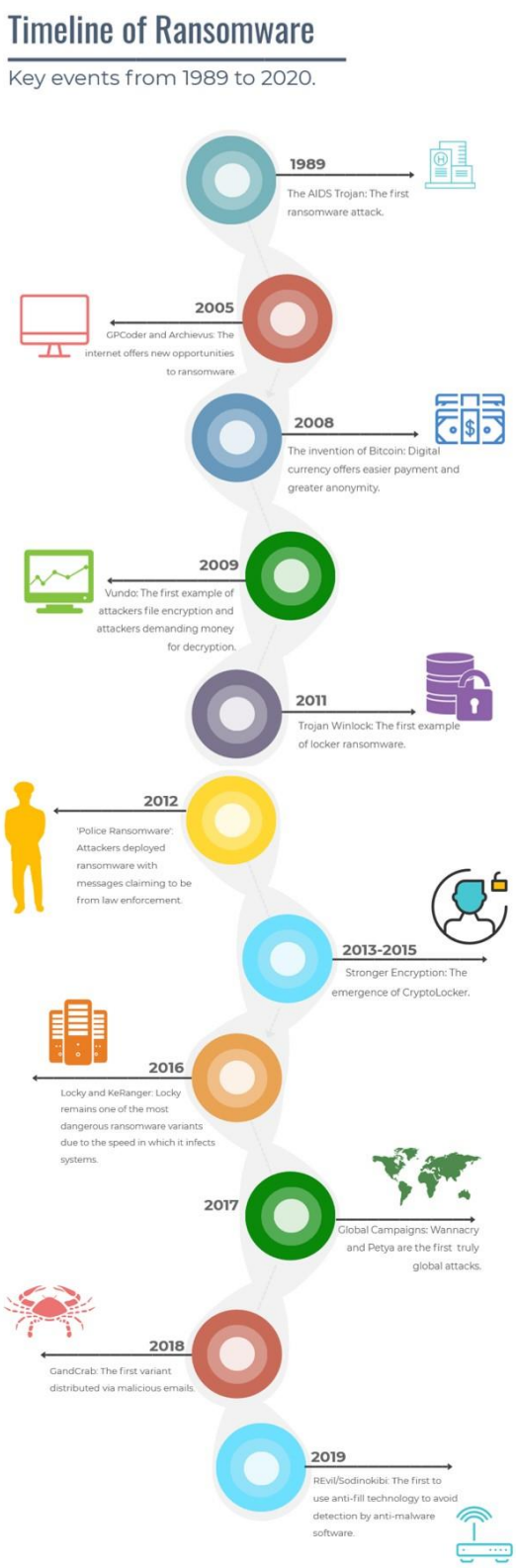

Figure 1. **A timeline of ransomware evolution.** *Made with Visme Infographic Maker.*

Sources

"A History of the Ransomware Threat: Past, Present, and Future." *vpn Mentor.* 2020. **https://www.vpnmentor.com/blog/history-ransomware-threat-past-present-and-future/**.

Agrawal, Neeraj. "Why ransomware criminals use Bitcoin and why that could be undoing." Coin Center. May 2017. **https://coincenter.org/link/why-ransomware-criminals-use-bitcoin-and-why-that-could-be-their-undoing**.

Ball, Tom. "The History of Ransomware." *Computer Business Review.* February 2018. **https://www.cbronline.com/news/the-history-of-ransomware**.

Bernard, Zoe. "Everything you need to know about Bitcoin, its mysterious origins, and the many alleged identities of its creator." *Business Insider.* November 2018. **https://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12**.

De Groot, Juliana. "A History of Ransomware." *Digital Guardian.* October 24, 2019. **https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time**.

Fuentes, Mark Anthony. "A Brief History of Ransomware." Horangi Cybersecurity. September 2019. **https://www.horangi.com/blog/a-brief-history-of-ransomware**.

"GandCrab." Malwarebytes. 2020. **https://www.malwarebytes.com/gandcrab/**.

"Locky Ransomware." KnowBe4. 2016. **https://www.knowbe4.com/locky-ransomware**.

"Ransomware." Cybersecurity and Infrastructure Security Agency. 2020. **https://www.us-cert.gov/Ransomware**.

"Ransomware." KnowBe4. 2020. **https://www.knowbe4.com/ransomware**.

"The Evolution of Ransomware: 2019 Brings the 30 Year Anniversary." Kraft, 2019. **https://kraftbusiness.com/cyber-security/evolution-of-ransomware-2019-brings-30-year-anniversary/**.

"The 10 Most Popular Types of Ransomware in 2019." Infotech News. January 2020. **https://meterpreter.org/the-10-most-popular-ransomware-in-2019/**.

Winder, Davey. "FBI Issues 'High-Impact' Cyber Attack Warning—What You Need to Know." *Forbes.* October 2019. **https://www.forbes.com/sites/daveywinder/2019/10/03/fbi-issues-high-impact-cyber-attack-warningwhat-you-need-to-know/#63af0e6740af**.

About the Author

Tess is a Client Success Manager at Kivu Consulting in Washington, DC. Tess has over five years' experience in security and intelligence. She specializes in helping customers navigate the ever-changing cyber security landscape and provides technical and product support to the managed service team through threat intelligence research. Tess's past work includes physical security and close protection, counter-terrorism intelligence analysis and research, and educational non-profit administration and management.

Tess Frieswick
tfrieswick@kivuconsulting.com

Threat Intel Reports

Kivu produces regular Threat Intel Reports using proprietary intelligence and publicly available information. Our aim is to provide easily digestible insight into cyber threat trends and threat actors' methods so that organizations can take actions to protect their networks and data.

About Kivu

Kivu is a leading global cyber security firm that offers a full suite of pre- and post-breach services, specializing in the forensic response to cyber-attacks and ransomware incidents. By combining analyst expertise, patented proprietary technology and exclusive threat intelligence, we deliver cutting edge cyber security solutions to organizations in need across the globe. Headquartered in the U.S. with offices worldwide, Kivu is a trusted cyber incident partner to insurance carriers and law firms.

kivuconsulting.com