THREAT INTEL REPORT

2019 Paid Ransomware Report

Overview

Ransomware is an attack that utilizes specialized malware to encrypt a victim's data files and entire computer systems. The attacker then demands a ransom payment from the victim to restore access to the data. Kivu clients that are victims of ransomware are presented with two options to proceed: pay the ransom or decline payment and either forfeit the data or restore from backups, or other sources.

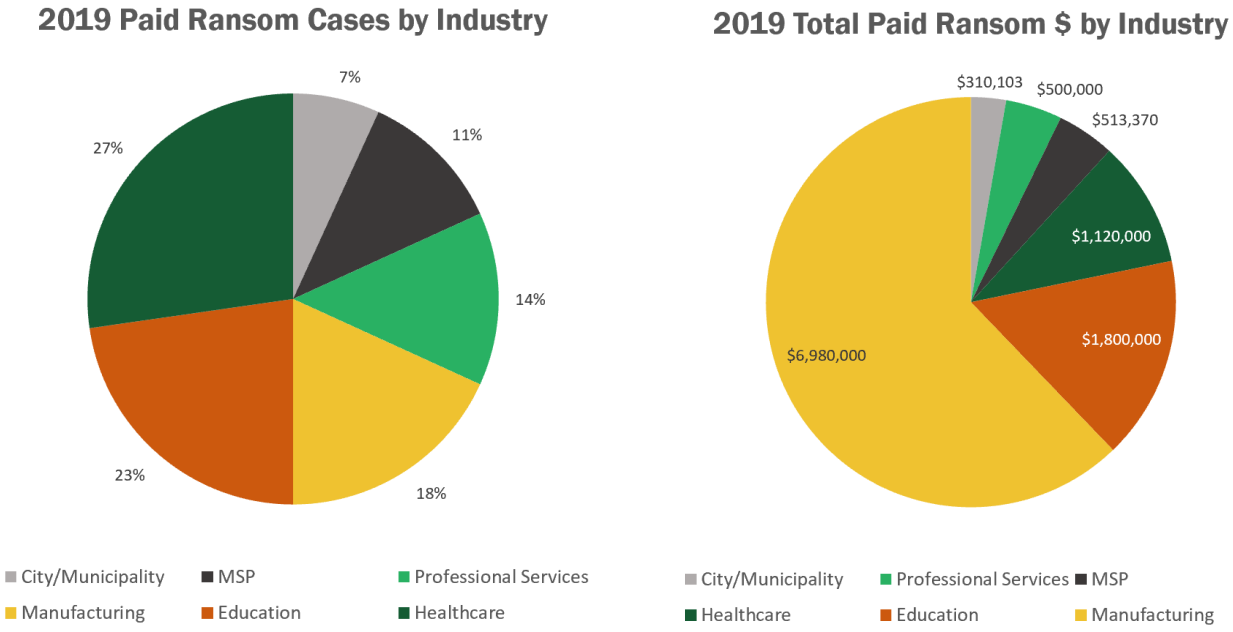
Kivu offers a full suite of pre- and post-breach services, specializing in the forensic response to cyber-attacks and ransomware incidents. Over the past four years, Kivu has been involved in over 700 ransomware incidents. In 2019, Kivu facilitated ransom payments in 143 cases, paying a total of over US$17m. This report uses data from 63 of those cases where the industry was identified and recorded, amounting to a total of over US$11m paid in ransom. It does not reflect cases where Kivu was able to assist clients without paying a ransom, or those where the victim's industry remained anonymous.

Ransomware: Everyone is a target

A common misconception is that ransomware attackers only target larger corporations and businesses.[1] In fact, attackers employ various tactics to target entities of all sizes in many industries.[2] State municipalities, education bodies, healthcare organizations, manufacturing companies and architecture firms comprise a few of the industries that Kivu assisted with ransomware payments in 2019.

---

[1] "Ransomware Attacks- Why It Should Matter To Your Business," *The National Review,* November 7, 2019, **https://www.natlawreview.com/article/ransomware-attacks-why-it-should-matter-to-your-business**
[2] "Ransomware Attacks- Why It Should Matter To Your Business," *The National Review.*



Paid Ransomware 2019 Breakdown

Education

The education industry comprised 23% of the overall paid ransomware cases Kivu managed in 2019. The total sum of education-related ransom payments reached $1,803,400. Victims included school districts, colleges and universities, and private and public schools. The average payment for school districts amounted to $132,287.67. The average payment for colleges and universities was $154,500, with the largest payment reaching $240,000.

The most common ransomware method utilized against these clients was Phobos. Phobos, named after the god of fear in Greek mythology, is a type of ransomware that is heavily based on Dharma (a.k.a. CrySis) and emerged in 2019.[3] Phobos is distributed via hacked Remote Desktop (RDP) connections.[4] Hacked RDP servers are a cheap and popular commodity on the

[3] "A deep dive in Phobos ransomware," *Malwarebytes Lab*, July 2019, **https://blog.malwarebytes.com/threat-analysis/2019/07/a-deep-dive-into-phobos-ransomware/**

[4] "A deep dive in Phobos ransomware," *Malwarebytes Lab*.

illicit underground market and represent a cost-effective attack vector for malicious actors.[5] Consequently, malware researchers assert that attackers who employ Phobos are less professional and not as organized as cybercriminal syndicates that build and distribute their own ransomware. This may result in longer negotiations, if the client decides to pay, and potential issues regarding the decryption of files and systems.[6]

Manufacturing

Despite only representing 18% of Kivu's paid ransom cases in 2019, manufacturing represented 62% of the +$11m in paid ransoms. The total amount of paid ransom for manufacturing clients reached $6,983,256 in the last year. The highest individual ransom payment was almost $2m. 67% of paid ransomware attacks against manufacturing clients were conducted via Ryuk. Ryuk is a type of crypto-ransomware that utilizes encryption to block access to a system, file or device until a ransom is paid.[7]

Cyber attackers target the manufacturing industry with ransomware to extort money, or steal intellectual property including: patents, formulas, schematics and blueprints.[8] A 2019 report found that the construction and manufacturing industries are the most targeted by ransomware globally, likely due to factors that make it difficult to invest in IT services or staff.[9] A Ponemon study estimates that production lines lose $22,000 an hour when production lines are halted.[10] These high costs impose significant pressure on businesses to quickly pay the ransom to restore business operations.

---

[5] Ibid.

[6] Stu Sjouwerman, "You Should Be Scared of the Latest Strands of Phobos Ransomware," *KnowBe4*, 2019, **https://blog.knowbe4.com/you-should-be-scared-of-the-latest-strains-of-phobos-ransomware**

[7] "Fall 2019 Threat of the Quarter: Ryuk Ransomware," *Center for Internet Security,* 2019, **https://www.cisecurity.org/white-papers/fall-2019-threat-of-the-quarter-ryuk-ransomware**

[8] Ellen Rosen, "Manufacturers Remain Slow to Recognize Cyber Risks," *The New York Times,* November 2018, **https://www.nytimes.com/2018/11/21/business/manufacturers-remain-slow-to-recognize-cybersecurity-risk.html**

[9] "Construction industry top target for ransomware attacks," *Inside Construction*, October 2019, **https://www.insideconstruction.com.au/news/latest-news/construction-industry-top-target-for-ransomware-attacks/**

[10] James Slaby, "Ransomware Targets Another Manufacturing Industry Target," *Acronis,* June 2019, **https://www.acronis.com/en-us/blog/posts/ransomware-crushes-another-manufacturing-industry-target**

Healthcare

27% of Kivu's paid ransom cases in 2019 were from clients in the healthcare industry, with an average payment of $87,106. Kivu's paid ransom cases were mostly comprised of small medical practices and clinics. 21% of the cases were executed with Crysis/Dharma ransomware. Another 21% of cases were conducted via Mr. Dec ransomware. Mr. Dec is a Trojan encrypted ransomware that is commonly distributed through spam emails with infected attachments.[11] Cyber-attacks against healthcare organizations are becoming increasingly popular as ransomware attacks against the industry rose 350% in the fourth quarter of 2019.[12] Most recently, attackers have been capitalizing on the disruption to and pressure on the healthcare system caused by the COVID-19 pandemic.[13]

Professional Services

Kivu saw a trend of attacks against architectural firms appearing in June 2019. The average payment made by Kivu's clients in the architecture industry was $68,893. 88% of ransomware attacks against Kivu's architecture clients that paid ransom were conducted via REvil, also known as Sodinokibi. Experts first identified REvil in April 2019.[14] At that time, REvil launched attacks via exploitation of Oracle WebLogic vulnerabilities. Threat actors have since expanded delivery to include malicious spam campaigns, RDP attacks, and other attack vectors.[15] REvil can perform the following tasks: exploit the CVE-2018-8453 vulnerability to elevate privileges, terminate blacklisted processes prior to encryption to eliminate resource conflicts, wipe the contents of blacklisted folders, encrypt non-whitelisted files and folders on local storage devices and network shares, and exfiltrate basic host information.[16]

> 88% of ransomware attacks against Kivu's architecture clients that paid ransom were conducted via REvil.

[11] "Mr.Dec Ransomware," EnigmaSoft, 2019, **https://www.enigmasoftware.com/mrdecransomware-removal/**

[12] Jessica Davis, "Ransomware Attacks on Healthcare Providers Rose 350% in Q4 of 2019," *Cybersecurity News*, March 2020, **https://healthitsecurity.com/news/ransomware-attacks-on-healthcare-providers-rose-350-in-q4-2019**

[13] Lindsey O'Donnell, "Cyberattacks Target Healthcare Orgs on Coronavirus Frontlines," *threat post*, April 14, 2020, **https://threatpost.com/cyberattacks-healthcare-orgs-coronavirus-frontlines/154768/**

[14] "REvil/ Sodinokibi," *Secureworks,* September 24, 2019, **https://www.secureworks.com/research/revil-sodinokibi-ransomware**

[15] "REvil/ Sodinokibi," *Secureworks.*

[16] Ibid.

MSSP/City and Municipalities

While MSSPs are generally a secure means of managing data and business operations, as with all service providers, they are not exempt from cyber-crime. In fact, 11% of paid ransom cases were paid on behalf of Managed Service Security Provider (MSSP) clients in 2019. The Sodinokibi/REvil ransomware methodology comprised 86% of these ransomware attacks. MSSP ransom payments peaked at $277,000. The average ransom payment for MSSP clients amounts to $85,562.

City and municipality related clients comprised 7% of paid ransom cases. 50% of these cases were conducted via Sodinokibi/REvil. The highest payment in this category was $223,000. The average payment in this category stood at $77,526.

Ransomware costs and facts:

- An organization fell victim to ransomware every 14 seconds in 2019.[17]
- 1.5 million phishing sites are created each month.[18]
- Companies are facing an average downtime of 9.6 days after being infected with ransomware.[19]
- The average ransomware payment for Kivu's clients was $123,037.56 in 2019.
- Downtime costs are typically five to 10 times the actual ransom amount, as measured by business interruption and company reputation.[20]

A ransomware attack could also incur the loss of customers, a diminished reputation, and increase in employee frustration.

---

[17] Colin R. Jennings, Ericka A. Johnson, Shalin A. Sood, "Ransomware Attacks- Why It Should Matter To Your Business," *The National Review*, November 2019, **https://www.natlawreview.com/article/ransomware-attacks-why-it-should-matter-to-your-business**

[18] Colin R. Jennings, Ericka A. Johnson, Shalin A. Sood, "Ransomware Attacks- Why It Should Matter To Your Business," The National Review.

[19] Ibid.

[20] Ibid.

How can organizations protect themselves from a ransomware attack?

One of the ways to minimize the risk of a ransomware attack is to invest in Managed Detection and Response (MDR) services. MDR functions as an extension of in-house IT teams by providing 24x7x365 managed endpoint detection security. This round-the-clock coverage is crucial, as 76% of all ransomware infections in the enterprise sector occur outside working hours.[21] 49% of weekend infections took place at night and 27% occurred during the day.[22] Endpoint protection allows cyber security analysts to prevent the installation of malware and remediate and hunt threats that enter a network or environment. **Kivu offers MDR services** as a cost-effective means to protect organizations from the financial and reputational costs of a security breach.

[21] "Most ransomware attacks take place during the night or over the weekend," *ZD Net*, March 2020, **https://www.zdnet.com/article/most-ransomware-attacks-take-place-during-the-night-or-the-weekend/**

[22] "Most ransomware attacks take place during the night or over the weekend," *ZD Net*.

Sources

“A deep dive in Phobos ransomware.” Malwarebytes Lab. July 2019. **https://blog.malwarebytes.com/threat-analysis/2019/07/a-deep-dive-into-phobos-ransomware**

“Construction industry top target for ransomware attacks.” Inside Construction. October 2019. **https://www.insideconstruction.com.au/news/latest-news/construction-industry-top-target-for-ransomware-attacks/**

Davis, Jessica. “Ransomware Attacks on Healthcare Providers Rose 350% in Q4 of 2019.” Cybersecurity News. March 2020. **https://healthitsecurity.com/news/ransomware-attacks-on-healthcare-providers-rose-350-in-q4-2019**

“Fall 2019 Threat of the Quarter: Ryuk Ransomware.” *Center for Internet Security.* 2019 **https://www.cisecurity.org/white-papers/fall-2019-threat-of-the-quarter-ryuk-ransomware/**

Jennings, Colin R., Ericka A. Johnson, Shalin A. Sood. “Ransomware Attacks- Why It Should Matter To Your Business.” The National Review. November 2019. **https://www.natlawreview.com/article/ransomware-attacks-why-it-should-matter-to-your-business**

”Most ransomware attacks take place during the night or over the weekend.” ZD Net. March 2020. **https://www.zdnet.com/article/most-ransomware-attacks-take-place-during-the-night-or-the-weekend/**

“Mr.Dec Ransomware.” EnigmaSoft. 2019. **https://www.enigmasoftware.com/mrdecransomware-removal/**

O’Donnell, Lindsey. “Cyberattacks Target Healthcare Orgs on Coronavirus Frontlines.” threat post. April 14, 2020. **https://threatpost.com/cyberattacks-healthcare-orgs-coronavirus-frontlines/154768/**

“Ransomware Attacks- Why It Should Matter To Your Business.” The National Review. November 7, 2019. **https://www.natlawreview.com/article/ransomware-attacks-why-it-should-matter-to-your-business**

“REvil/ Sodinokibi.” *Secureworks.* September 24, 2019. **https://www.secureworks.com/research/revil-sodinokibi-ransomware**

Rosen, Ellen. “Manufacturers Remain Slow to Recognize Cyber Risks.” *The New York Times.* November 2018. **https://www.nytimes.com/2018/11/21/business/manufacturers-remain-slow-to-recognize-cybersecurity-risk.html**

Slaby, James. “Ransomware Targets Another Manufacturing Industry Target.” *Acronis.* June 2019. **https://www.acronis.com/en-us/blog/posts/ransomware-crushes-another-manufacturing-industry-target**

Sjouwerman, Stu. “You Should Be Scared of the Latest Strands of Phobos Ransomware.” KnowBe4. 2019. **https://blog.knowbe4.com/you-should-be-scared-of-the-latest-strains-of-phobos-ransomware**

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' 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 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