CYBERDEFENSE REPORT

From Ransomware to Ransom War
The Evolution of a Solitary Experiment into Organized Crime

Max Smeets

Zürich, September 2024
Center for Security Studies (CSS), ETH Zürich

CSS
ETH Zürich

ETH zürich

Available online at: https://css.ethz.ch/en/publications/risk-and-resilience-reports.html

Author: Max Smeets

ETH-CSS project management: Stefan Soesanto, Project Lead Cyberdefense; Andreas Wenger, Director of the CSS.

Editor: Eugenio Benincasa, Senior Cyberdefense Researcher, CSS

DOI: 10.3929/ethz-b-000692241

Table of Content

1 Introduction

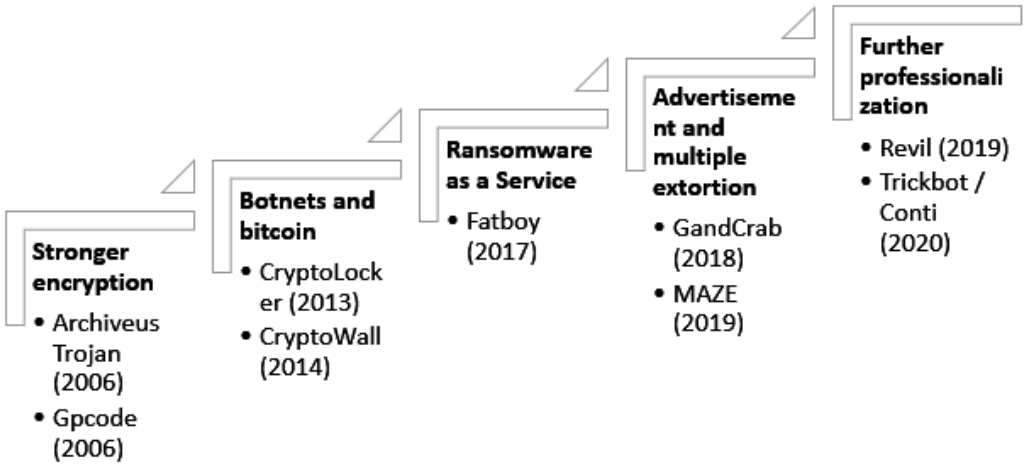
This report is based on chapter one of Max Smeets' book titled "Ransom War: How Cyber Crime became a Threat to National Security," forthcoming with *Oxford University Press* and *Hurst Publishers.*

Historically, discussions on cyber conflict have primarily centered on the involvement of state-sponsored or affiliated groups.[1] Yet, the growing prominence of criminal actors – specifically, ransomware groups – now demands a shift in attention. Ransomware, a type of malicious activity where hackers lock access to files or systems until a ransom is paid, increasingly threatens both citizen safety and global stability. In 2022, the majority of the U.K's government's crisis management "Cobra" meetings were convened in response to ransomware incidents rather than other national security emergencies.[2] According to Sami Khoury, the head of the Canadian Center for Cyber Security, the threat from nation-states remains significant but cybercrime, of which ransomware is the most disruptive form, is "the number one cyber threat activity affecting Canadians."[3] The Swiss National Cybersecurity Centre warns that ransomware could pose an "existential threat" to businesses and government agencies.[4]

This report discusses significant milestones in the development of ransomware, and what turned them into a significant threat to human and national security.[5]

It starts with the adoption of better encryption techniques by criminals, enabling them to effectively hold data for ransom. The use of botnets subsequently expanded their operational reach, while there was also a shift away from prepaid card systems in favor of cryptocurrencies such as Bitcoin, which provided anonymity and ease of transaction. Following these developments, the emergence of Ransomware as a Service (RaaS) allowed for a better division of tasks within the cybercriminal community, making it easier for newcomers to participate. Tactics evolved further to include double extortion, where attackers threaten to publish stolen data unless a ransom is paid. The final shift saw the professionalization of ransomware groups. It also increased their intent and capability to target major organizations, maximizing their ransom potential. I refer to the ransomware groups at the forefront of this troubling trend in the criminal ecosystem as *ransom war groups*.

Figure 1: The Development of Ransomware



Source: Compiled by Max Smeets

[1] For a discussion on the change in discourse, see: Chesney & Smeets, eds. *Deter, Disrupt, or Deceive*, Georgetown University Press, 2023

[2] Alexander Martin, "Ransomware Incidents Now Make up Majority of British Government's Crisis Management 'Cobra' Meetings," *The Record*, November 18, 2022, https://therecord.media/ransomware-incidents-now-make-up-majority-of-british-governments-crisis-management-cobra-meetings

[3] Canadian Centre for Cyber Security, "National Cyber Threat Assessment 2023-2024," October 28, 2022, https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024

[4] National Cyber Security Centre (NCSC), "Ransomware", 2024, https://www.ncsc.admin.ch/ncsc/en/home/cyberbedrohungen/ransomware.html

[5] For discussion on some of the general technological drivers for cyber crime and ransomware see: Matthew Ryan, *Ransomware Revolution: The Rise of a Prodigious Cyber Threat*, Springer, 2021

2 The First Ransomware Incident

In June 1988, the fourth International AIDS Conference convened in Stockholm, Sweden. Distinguished attendees, including senior government representatives, academics, and other leading experts, converged at this event to examine the epidemiology, clinical management, and preventive strategies related to this pressing public health issue.[6]

About a year later, the attendees of the conference received a peculiar mailing: a floppy disk labelled "AIDS Information Introductory Diskette Version 2.0." This same floppy disk found its way to the subscribers of a prominent London-based magazine, *PC Business World.*[7] The floppy disk appeared to contain an interactive software program called "AIDS Information." The program inquired about the respondents' habits and medical histories, and subsequently calculated the risks associated with contracting AIDS. For those respondents categorized as high-risk, the program spared no words, spitting out a warning message you would now see on the back of cigarette packages: "Your behavior patterns are extremely dangerous and they will very likely kill you."[8]

However, unbeknownst to the recipients, the floppy disk also contained a malicious program that infected AUTOEXEC.BAT, a DOS and early Windows system file that runs commands automatically at startup to configure the system environment. The virus did not affect the computer's booting process, but counted the number of times the computer was powered on. Once a specific threshold, typically 90 times, was crossed, the malware sprang into action, encrypting the names of all the files on the main hard drive. The price tag for unlocking the files on the device came in two flavors: a temporary lease for 189 USD or a purportedly lifetime lease for 379 USD. The displayed message, the first ever-recorded ransomware notice to victims, read as follows:

```
Dear Customer:

It is time to pay for your software lease
from PC Cyborg Corporation.
Complete the INVOICE and attachment for the
lease option of your choice.
If you don't use the printed INVOICE, then
be sure to refer to the important reference
numbers below in all correspondence. In re-
turn you will receive:

- a renewal software package with easy-to-
follow, complete instructions;
- an automatic, self-installing diskette
that anyone can apply in minutes.

Important reference numbers: [...]

The price of 365 use application is US$189.
The price of a lease for the lifetime of
your hard disk is US$378. You must enclose
a bankers draft, cashier's check or inter-
national money order payable to PC CYBORG
CORPORATION for the full amount of $189 or
$379 with your order. Include your name,
company, address, city, state, country, zip
or postal code. Mail your order to PC Cyborg
Corporation, P.O. Box 87-17-44, Panama 7,
Panama.

          Press ENTER to continue
```

The programs were written by Joseph L. Popp, who received a doctorate in evolutionary biology and had studied at Harvard University. He spent much of his life living in various African countries.[9] With this message appearing on the screen, Popp presented the computer lock as a voluntary licensing agreement in an attempt to stay within the bounds of the law. He tried to make the case that users of the AIDS program would bear full responsibility for any computer freezes, as his license agreement explicitly warned that failure to make the payment could "adversely affect" the computer.[10]

Popp had set up an elaborate scheme to receive the money. A cheque, bankers transfer, or international money order had to be sent in an envelope to a post office box in Panama, payable to PC CYBORG CORPORATION. Yet, the malware relied on symmetrical encryption, a type of encryption that employed a single secret key for both data encryption and decryption, rendering it relatively easy to decrypt. Soon after the release of the virus, security researcher Jim Bates was the first to produce a

[6] "AIDS 88 Summary: A Practical Synopsis of the IV International Conference, Stockholm, Sweden," NCJRS Virtual Library, 1988, https://www.ojp.gov/ncjrs/virtual-library/abstracts/aids-88-summary-practical-synopsis-iv-international-conference

[7] Edward Wilding, "The Authoritative International Publication on Computer Virus Prevention, Recognition and Removal," *Virus Bulletin*, January 1992, https://www.virusbulletin.com/uploads/pdf/magazine/1992/199201.pdf.

[8] See: Renee Dudley & Daniel Golden, *The Ransomware Hunting Team: A Band of Misfits' Improbable Crusade to Save the World from Cybercrime*, Farrar, Straus and Giroux, 2022; David Ferbrache, *A Pathology of Computer Viruses*, Springer Science & Business Media, 1992

[9] Aimee Bosman, "First Ransomware: Joseph L. Popp," *LinkTek.com*, February 19, 2024, https://linktek.com/malice-money-monkeys-and-a-madman-the-origin-of-ransomware/

[10] Renee Dudley & Daniel Golden, *The Ransomware Hunting Team: A Band of Misfits' Improbable Crusade to Save the World from Cybercrime*, Farrar, Straus and Giroux, 2022

reliable removal and retrieval program from the victims.[11] The two programs were distributed free of charge providing much-needed relief to those impacted.

Only those who panicked and wiped their own data suffered lasting harm. Tragically, a university in Milan permanently erased ten years of astronomical observations, and an AIDS research center in Bologna lost a decade's worth of critical data. None of Popp's victims were known to have made any payments. Ironically, Popp's only income came from the Computer Crime Unit of Scotland Yard's Fraud Squad, who sent the fee during their investigation. PC CYBORG CORPORATION failed to fulfill their claim of providing a decryption tool.

To attribute the AIDS virus to Joseph Popp, Scotland Yard relied on several conventional investigative techniques. PC CYBORG CORPORATION's establishment was traced back to a phone call from Addis Ababa, Ethiopia, where an individual identifying as "Elizabeth Ketema" claimed responsibility. This same person had procured a mailing list from a Nigerian software company for 2.000 USD. The investigators observed a remarkable resemblance in appearance and handwriting between Ketema and Popp. Investigators uncovered additional evidence pointing to Popp as the culprit. Popp's fingerprints were discovered on both the disks and inside several envelopes, each adorned with postmarks from London's Kensington area – an area not far from Popp's residence during that period. Moreover, antigen testing of the saliva from the stamps used to mail the floppy disks aligned with a sample obtained from Popp at a later stage.[12]

After the FBI seized Popp's computer, containing the AIDS program's programming, the British government requested his extradition. Popp claimed psychiatric medication hindered his understanding of the proceedings, and specialists examined him.[13] Upon his arrival in England, Popp's conduct became progressively bizarre. The *Virus Bulletin*, a computer magazine, wrote that Popp's "recent antics have included wearing a cardboard box, putting hair rollers in his beard to protect himself from 'radiation' and 'micro-organisms' and wearing condoms on his nose."[14] While some psychiatric professionals diagnosed him with severe mental illness, not all concurred with this evaluation. His bizarre conduct in England raised enough concern that he was deemed unfit for trial in November 1991. Eventually, Popp established a butterfly conservatory in Oneonta, New York.[15]

3 Towards Stronger Encryption

The foundational success of any extortion effort lies in eliminating all avenues of escape for the victim. At the core of this use of ransomware is the deployment of strong encryption, which effectively locks victims' data or computer systems, compelling payment for its release, without alternative escape. While the knowledge for implementing strong encryption had been available for quite some time, its widespread adoption by ransomware groups took several years to materialize.

The year 2006 witnessed a significant milestone with the introduction of the Archiveus Trojan. Once a computer fell victim to Archiveus, it copied all files from the user's "My Documents" folder into a single file called EncryptedFiles.als, encrypting them in the process.[16] Archiveus subsequently removed the original files, leaving only the encrypted copy behind. Archiveus was the first to employ the asymmetric encryption method known as RSA. The RSA algorithm, named after its creators Ron Rivest, Adi Shamir, and Leonard Adleman from the Massachusetts Institute of Technology, was publicly described for the first time in 1977.[17] Unlike the symmetric encryption used by Popp, RSA's asymmetric encryption involves one public

[11] Edward Wilding, "The Authoritative International Publication on Computer Virus Prevention, Recognition and Removal," *Virus Bulletin*, March 1990, https://www.virusbulletin.com/uploads/pdf/magazine/1990/199003.pdf;

[12] Renee Dudley & Daniel Golden, *The Ransomware Hunting Team: A Band of Misfits' Improbable Crusade to Save the World from Cybercrime*, Farrar, Straus and Giroux, 2022

[13] Ibid.

[14] Edward Wilding, "The Authoritative International Publication on Computer Virus Prevention, Recognition and Removal," *Virus Bulletin*, March 1990, https://www.virusbulletin.com/uploads/pdf/magazine/1990/199003.pdf

[15] While Popp was in a psychiatric hospital, he was overheard on the telephone bragging to someone that he had deceived the system to evade trial. The Southwark judge, however, did believe Popp's claim. See: Renee Dudley & Daniel Golden, *The Ransomware Hunting Team: A Band of Misfits' Improbable Crusade to Save the World from Cybercrime*, Farrar, Straus and Giroux, 2022

[16] Jennifer LeClaire, "Sophos Cracks Archiveus Ransomware Code," *TechNewsWorld*, June 2, 2006, https://www.technewsworld.com/story/sophos-cracks-archiveus-ransomware-code-50881.html; Cary Kostka, "What Is Archiveus Trojan? A Part of the History of Modern Ransomware," *Ransomware.org*, February 23, 2022, https://ransomware.org/blog/archiveus-trojan-a-part-of-the-history-of-modern-ransomware/

[17] Already in 1973 British mathematician Clifford Cocks created a public key algorithm, but it was kept classified by the UK's GCHQ until 1997. Also see: Cryptome, "The Alternative History of Public-Key Cryptography," accessed on May 4, 2024, https://cryptome.org/ukpk-alt.htm; Based on Simon Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Random House, 1999, pp. 279–92

key and one private key. The public key can be shared openly, while the private key must be kept secret. RSA allows data to be encrypted using either the public or private key, with the opposite key used for decryption. RSA's encryption security lies in the challenge of factoring large integers resulting from two large prime numbers. While multiplying these numbers is simple, factoring them back into the original primes is considered very challenging.

Popp pretended the customer had to pay for a software lease, as a social engineering technique to coerce victims into paying the ransom. Archiveus applied a different technique to apply more pressure on the victim. When victims of Archiveus tried to access their encrypted files they were directed to a text file with instructions on how to regain access to the data.[18] The instructions falsely accused victims of visiting illegal porn sites, likely to embarrass them and dissuade them from seeking external assistance.[19] The instruction goes on to state "Do not try to search for a program that encrypted your information - it simply does not exist in your hard disk anymore. Reporting to police about a case will not help you, they do not know the password. Reporting somewhere about our e-mail account will not help you to restore files. Moreover, you and other people will lose contact with us, and consequently, all the encrypted information."[20]

Whereas Popp never provided a decryption tool to its sole payer, the victims from Archiveus did receive a long password from the hackers to decrypt the files after they made a purchase from specified online pharmacies. However, flaws in Archiveus' encryption meant that even with the password, victims often still lost their files.[21]

Around the same period, other cybercriminals were exploring the use of RSA encryption. An example was GPCode, which targeted Windows users through spear-phishing emails. These emails, seemingly from reputable Western companies, offered attachments with enticing details on salary and benefits, sourced from job.ru, a major Russian job portal. The catch wasn't immediate; opening the attachment would install a malware that later downloaded GPCode, effectively masking the initial source of infection and leaving many unaware of the true entry point of the ransomware.

The first instances of GPCode were detected by Kaspersky Lab in December 2004. They noticed that GPCode predominantly targeted Russian businesses such as banks, advertising firms, and real estate agencies, employing basic encryption techniques. By June 2005, a second outbreak also targeted almost exclusively Russian entities, attempting to deploy a more complex encryption algorithm, which, nonetheless, security experts managed to decrypt with relative ease. [22]

However, in early 2006, a significant shift occurred. It appeared that the creator of GPCode had spent some time studying encryption – possibly drawing inspiration from Archiveus – to release a new variant of GPCode using RSA encryption algorithms.[23] As the ransomware evolved, the encryption key became progressively longer. It began with a 56-bit key, then advanced to 67 bits, followed by a 260-bit RSA key, a 330-bit key, and finally reaching a 660-bit key with the release of version Gpcode.ag on July 4, 2006. This progression in key length significantly complicated the decryption process for those trying to assist the victims.

Despite the greater sophistication of the encryption, the ransom demands remained modest, starting at 2.000 rubles (about 70 USD at the time) and even decreasing to 500 rubles (approximately 20 USD). The tactic behind Archiveus was not to amass large sums from individual victims but to capitalize on the volume of payments.

Today, an unspoken understanding prevails that ransomware operators refrain from targeting the Common-

[18] TechNewsWorld, "Sophos Cracks Archiveus Ransomware Code," June 2, 2006, https://www.technewsworld.com/story/sophos-cracks-archiveus-ransomware-code-50881.html

[19] In later years, it became common for ransomware to masquerade as law enforcement agencies, falsely accusing users of illegal activities online and demanding payment of a fine. This type of ransomware is termed 'scareware.' A prominent example is the Reveton ransomware, which emerged in 2012. It displayed a message claiming to be from United States law enforcement, alleging that the user had engaged in activities such as using pirated software or accessing child pornography. In some cases, Reveton would activate the victim's camera to suggest that a recording was being made. KnowBe4, "Reveton Worm Ransomware," accessed May 4, 2024, https://www.knowbe4.com/reveton-worm; Jonathan Reed, "How Reveton Ransomware-as-a-Service Changed Cybersecurity," *Security Intelligence*, December 19, 2022, https://securityintelligence.com/articles/how-reveton-raas-changed-cybersecurity/; Marlese Lessing, "Case Study: Reveton Ransomware," *SDX Central*, accessed May 4, 2024, https://www.sdxcentral.com/security/definitions/what-is-ransomware/case-study-reveton-ransomware/

[20] Jon Stewart, "Archiveus Ransomware Trojan Threat Analysis," Secureworks, May 5, 2006, https://www.secureworks.com/research/arhiveus

[21] Researchers from the cybersecurity firm Sophos eventually identified and disclosed the decryption key, mitigating the damage inflicted by the ransomware. See: Cary Kostka, "What Is Archiveus Trojan? A Part of the History of Modern Ransomware," Ransomware.org, February 23, 2022, https://ransomware.org/blog/archiveus-trojan-a-part-of-the-history-of-modern-ransomware/

[22] Denis Nazarov & Olga Emelyanova, "Blackmailer: The Story of Gpcode," *SecureList*, June 26, 2006, https://securelist.com/blackmailer-the-story-of-gpcode/36089/

[23] "The proud blackmailer even created a website; effectively 'RSA for dummies.'" See: Nazarov & Emelyanova, "Blackmailer: The Story of Gpcode."

wealth of Independent States (CIS), a regional organization formed during the dissolution of the Soviet Union with primarily former Soviet Republics. It is the region known for hosting the majority of these attacks.[24] As a consequence, law enforcement in the CIS region tends to ignore their activities. However, GPCode's history demonstrates that this rule was not always in place; it emerged and solidified as the cybercrime community evolved over time.[25]

4 Botnets and Bitcoin

During the early 2000s, ransomware had not yet become a dominant form of cybercrime, overshadowed by more lucrative activities like trafficking in stolen credit cards, passports and other documents. This era, spanning the late 1990s and early 2000s, coincided with the internet becoming mainstream and the rise of social media and online entertainment platforms. It was during this period that a North American group launched Counterfeit Library in 2000, initially as a space for victims of scams to share their experiences.[26] However, it quickly evolved into a marketplace for counterfeit documents.

Meanwhile, the Russian-speaking cybercriminal community saw the advent of CarderPlanet in 2001, marking a significant milestone in the evolution of cybercrime.[27] CarderPlanet distinguished itself (from Counterfeit Library) by becoming the first global cybercrime marketplace, recognized for its organized structure and adherence to a strict hierarchy, drawing inspiration from the ranks of the Sicilian Mafia – a nod to the influence of "The Godfather."[28] This platform laid the groundwork for the carding market's expansion over the next decade, leading to the emergence of numerous sites dedicated to these illegal exchanges.

Ransomware only began to carve its niche in the cybercriminal world in the mid-2000s with the introduction of new variants that simplified targeting and opened direct paths to financial exploitation. A significant breakthrough came in 2013 with the appearance of CryptoLocker, which introduced several innovations.[29] CryptoLocker was the first ransomware to rely on a botnet infrastructure, specifically the Gameover Zeus botnet, for distribution. A botnet infrastructure refers to a network of infected computers, controlled remotely to execute coordinated attacks without the users' knowledge. This botnet propagated through spam emails, leading to the download of malware that enabled hackers to perform a range of malicious activities, including disabling system processes, stealing banking information, and installing the CryptoLocker ransomware.

Another key distinction of CryptoLocker was its encryption strategy, employing 2048-bit RSA key pairs – far surpassing the complexity of 660-bit key used by GPCode and rendering brute-force decryption attempts futile.[30] In certain versions of CryptoLocker, failing to meet the initial ransom deadline allowed victims a second chance to retrieve their files at a significantly higher cost, with ransom amounts fluctuating across different versions and currencies.[31]

The final aspect that makes CryptoLocker stand out is that payments could not only be made with prepaid card systems like Paysafecard and Moneypak, but also by Bitcoin. Initially, prices were established at 100 USD, 100 EUR, 100 GBP, two Bitcoins, or similar amounts for different currencies. Some reports suggest that 41.928 Bitcoins circulated through four Bitcoin accounts linked to CryptoLocker,

[24] According to Chainalysis, since 2020, more than 90% of ransom payments associated with significant ransomware strains have been traced to ransomware that is deliberately programmed to exclude victims from the CIS. See: Chainalysis, "Eastern Europe's Crypto Crime Landscape: Scams Dominate, Plus Significant Ransomware Activity," October 14, 2021, https://www.chainalysis.com/blog/eastern-europe-cryptocurrency-geography-report-2021-preview/

[25] "Users found their files encrypted, and it was unclear which program had been used for encryption. The only clue left by the virus, aside from the encrypted files, was a text file named !Vnimanie!.txt ('vnimanie' translates to 'attention' in Russian). This file suggested the virus's Russian origins, as both the file name and the text within were in Russian. Additionally, some of the encrypted file formats were almost exclusively used in Russia, further pointing to the source of the virus. See: Nazarov & Emelyanova, "Blackmailer: The Story of Gpcode."

[26] Jonathan Lusthaus, *Industry of Anonymity: Inside the Business of Cybercrime*, Harvard University Press, 2018

[27] It was the brainchild of a Ukrainian cybercriminal known as Script, who had taken inspiration from the likes of carder.org and carder.ru. The origins of CarderPlanet are shrouded in myth, fueled in part by rumors that the key players met in person and convened a cybercrime convention in Odessa, Ukraine. See: Jonathan Lusthaus, *Industry of Anonymity: Inside the Business of Cybercrime*.

[28] Script was influenced by The Godfather. See: Jonathan Lusthaus, *Industry of Anonymity: Inside the Business of Cybercrime*, Harvard University Press, 2018, p.43-44

[29] Ryan W. Neal, "CryptoLocker Virus Holds Computers For Ransom," *International Business Times*, October 21, 2013, https://www.ibtimes.com/cryptolocker-virus-new-malware-holds-computers-ransom-demands-300-within-100-hours-threatens-encrypt; Bleeping Computer, "CryptoLocker Ransomware Information Guide and FAQ," October 14, 2013, https://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information

[30] Kurt Baker, "History of Ransomware," CrowdStrike, October 10, 2022, https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/

[31] This was not the first time this happened. A previously instance was Jigsaw.

translating to over 27 million USD in payments based on the Bitcoin value at the time.[32] That is over 3 billion USD in Bitcoin value as of March 2024.

The infrastructure for CryptoLocker's distribution, the Gameover Zeus botnet, was masterminded by Evgeniy Mikhailovich Bogachev. Recognized as a high-value target, the FBI has offered a reward of up to 3 million USD for information that could lead to Bogachev's arrest or conviction. He was "last known to reside in Anapa, Russia" and "is known to enjoy boating and may travel to locations along the Black Sea in his boat."[33]

A collaborative international effort eventually led to the dismantling of the Gameover Zeus and CryptoLocker operations. In a public statement, U.S. Assistant Attorney General Caldwell stressed the complexity of cybercriminal operations like Gameover Zeus and CryptoLocker, noting the successful disruption of these networks through a collaborative effort involving international and private sector partners: "These schemes were highly sophisticated and immensely lucrative, and the cyber criminals did not make them easy to reach or disrupt […]. But under the leadership of the Justice Department, U.S. law enforcement, foreign partners in more than 10 different countries and numerous private sector partners joined together to disrupt both these schemes. Through these court-authorized operations, we have started to repair the damage the cyber criminals have caused over the past few years, we are helping victims regain control of their own computers, and we are protecting future potential victims from attack."[34] The FBI reported that Gameover Zeus compromised more than 250.000 computers, resulting in losses exceeding 100 million USD.

Within its mere seven months of operation, CryptoLocker left a profound impact on the cybercrime community. Its success served as undeniable evidence of the great profit potential within this form of cybercrime. Shortly after its emergence, security researchers encountered numerous CryptoLocker clones in the wild, prompting other criminals to join the fray, eager to take part in this lucrative enterprise.[35]

CryptoWall emerged as its most remarkable successor. During the period from mid-March to late August 2014, CryptoWall proliferated extensively via spam phishing emails, infecting a staggering number of over 600.000 computer systems. Its impact extended to the encryption of more than 5.25 billion files. Despite its widespread infection, only a small fraction of victims opted to pay the ransom. As per one report, merely 0.27 percent of victims, amounting to 1.683 individuals, opted to pay the ransom, which averaged around 500 USD, in order to receive the decryption key.[36]

Cybersecurity company CrowdStrike describes this period as "the true inflection point for ransomware's hockey-stick growth."[37] Developers in the criminal ecosystem established more specialized operations to craft better ransomware code and exploit kit components, flooding the underground hacking marketplaces with their nefarious offerings. With the specialized expertise of developers flowing from other parts of the cybercrime market towards ransomware, it was empowered to further proliferate and evolve into an increasingly formidable threat. This led to another development: Ransomware as a Service.

5 Ransomware as a Service

In the early 2000s, the emergence of Software as a Service (SaaS) began transforming how businesses operate by simplifying and reducing the cost of using software. Instead of purchasing and managing software on their own systems, companies could now subscribe to software services, eliminating the need for extensive installations and ongoing maintenance. This shift allowed businesses to access software remotely without significant investment in IT infrastructure, opening up access to advanced software solutions once exclusive to large corporations, even for smaller businesses.

[32] KnowBe4, "Reveton Worm Ransomware," https://www.knowbe4.com/reveton-worm

[33] FBI, "Most Wanted: EvGeniy Mikhailovich Bogachev," accessed on May 4, 2024, https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev

[34] United States Department of Justice, "U.S. Leads Multi-National Action Against 'Gameover Zeus' Botnet and 'Cryptolocker' Ransomware, Charges Botnet Administrator," Office of Public Affairs, June 2, 2014, https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware

[35] For more on the market changes see: Kurt Baker, "History of Ransomware," CrowdStrike, October 10, 2022, https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/

[36] KnowBe4, "CryptoWall Ransomware," accessed on May 5, 2024, https://www.knowbe4.com/cryptowall

[37] Kurt Baker, "History of Ransomware," CrowdStrike, October 10, 2022, https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/

By 2015, this SaaS model had evolved into a new variant used by ransomware groups, dubbed Ransomware as a Service (RaaS).[38] RaaS operates on a collaborative framework, delineating roles between the RaaS operator and affiliate. The operator supplies affiliates with the necessary tools, infrastructure, and support for conducting ransomware attacks. This includes recruiting affiliates via online forums, providing them with tailored ransomware packages, and setting up a command-and-control dashboard for campaign monitoring. Operators also manage victim payment portals and aid in ransom negotiations, sometimes extending technical support to ensure the affiliates' operations run smoothly.[39]

The affiliates are the ones executing the ransomware attacks. They gain access to the ransomware by paying the RaaS operator, which can be through a one-time fee, a subscription model, or a profit-sharing scheme based on the ransoms collected. It is common for affiliates to write the ransom notes and handle communications with the victims via chat services. Crucially, they normally manage the decryption keys, which are essential for unlocking the victims' data once the ransom is paid.[40]

RaaS offerings range from basic, cost-effective options to more sophisticated and expensive packages. An example of a low-cost ransomware variant was Stampado. It was offered on the dark web for just 39 USD, providing a lifetime license.[41] A pioneering example of RaaS aiming to minimize effort for affiliates was the Shark Ransomware Project, launched in mid-2016. Setting it apart from the typical ransomware hosted on the anonymous Tor network, Shark was accessible via a publicly available WordPress site. Affiliates simply needed to complete a form specifying their requirements to create customized ransomware. In return for facilitating this streamlined process, Shark's developers took a twenty percent cut of any ransom payments collected.[42]

Investors often emphasize the importance of scalability in business, distinguishing it from mere growth by its ability to increase revenue without corresponding increases in costs. This concept of scalability is crucial for venture capital firms when evaluating startups for potential funding. The advent of RaaS has dramatically demonstrated the power of scalability in the cyber criminal ecosystem. RaaS allows for the centralized development of easy-to-use interfaces and tools, like encryption generators, decryption software, and victim communication and monitoring platforms.[43] This model enables ransomware developers to amplify their reach and impact significantly without proportionately increasing their operational costs, thereby scaling their operations effectively.

6 Advertisement and Double Extortion

As RaaS emerged, the developers behind ransomware began to engage more openly on underground forums. By showcasing their services prominently, RaaS providers aimed to build trust and attract potential affiliates, relying on the principle that a prominent presence could bolster their credibility.[44] In March 2017, an individual using the alias “polnowz” posted an advertisement for “Fatboy,” a new RaaS offering, on a Russian criminal forum. “We invite you to take part in a partnership for the monetization of downloads with help of the Fatboy encryption software. Limited partnership,” the advertisement read.[45] It explained that purchasers of Fatboy would work directly with Polnowz, communicating through Jabber, an instant messaging platform, and receive immediate payment upon ransom receipt from victims. Fatboy's pricing strategy was notably based on the Big Mac Index, a concept

[38] RaaS was already applied for the first time in 2014. But grew further in the years after.

[39] For an overview of RaaS compared to earlier forms of ransomware, sometimes called 'commodity ransomware.' Also see: Kris Oosthoek et al. “A Tale of Two Markets: Investigating the Ransomware Payments Economy,” *Communications of the ACM*, 66(8), 2023, 74–83, https://doi.org/10.1145/3582489

[40] Also see: Adam Marget, “Ransomware-as-a-Service (RaaS): What It Is & How It Works,” *Unitrends*, August 5, 2022, https://www.unitrends.com/blog/ransomware-as-a-service-raas

[41] “New Stampado Ransomware Sold Cheap on the Dark Web,” *Trend Micro DE,* July 14, 2016, https://www.trendmicro.com/vinfo/de/security/news/cybercrime-and-digital-threats/new-stampado-ransomware-sold-cheap-on-the-dark-web; But it was also ineffective. See: Lawrence Abrams, “Stampado Ransomware Campaign Decrypted before It Started,” *BleepingComputer*, July 22, 2016, https://www.bleepingcomputer.com/news/security/stampado-ransomware-campaign-decrypted-before-it-started/

[42] On the distinctive approach in ransomware distribution of Shark: Lawrence Abrams, “The Shark Ransomware Project Allows You to Create Your Own Customized Ransomware,” *BleepingComputer*, August 15, 2016, https://www.bleepingcomputer.com/news/security/the-shark-ransomware-project-allows-to-create-your-own-customized-ransomware/

[43] Operators also devised engagement strategies, such as deactivating dormant affiliate accounts, to maintain a dynamic and active affiliate base. Also see: “CONTI Ransomware Group,” *PRODAFT*, accessed May 5, 2024, https://resources.prodaft.com/conti-ransomware-group-report

[44] Also see: Diana Granger, “Fatboy Ransomware-as-a-Service Emerges on Russian-Language Forum,” *Recorded Future*, May 4, 2017, https://www.recordedfuture.com/blog/fatboy-ransomware-analysis

[45] Ibid.

from *The Economist* used to gauge purchasing power of different currencies, meaning victims in higher cost-of-living regions would face steeper ransom fees.[46] The advertisement detailed other features such as a multilingual interface, automatic decryption post-payment, and a comprehensive partner panel, while also specifying non-operation in the Commonwealth of Independent States.[47,48]

Fatboy's detailed and public advertisement strategy was aimed at rapidly building trust within its criminal customer base. This trend of public, detailed advertisements for ransomware services was further amplified by GandCrab, which transformed ransomware into a media-centric business. GandCrab excelled in branding, marketing, outreach, and public relations, engaging continuously with customers, partners, victims, and security researchers to craft a new type of ransomware enterprise.[49]

Offering a user-friendly RaaS model, GandCrab attracted novices to the field, who, as they became more adept, contributed to the evolution of GandCrab's techniques and eventually launched their own ransomware initiatives. This resulted in a swift development cycle for GandCrab, with the malware undergoing constant updates to bypass security measures.[50] By January 2018, GandCrab had seen at least five major updates, introducing new features and bug fixes that posed significant challenges for the cybersecurity community to mitigate.[51]

An important figure in GandCrab's affiliate program was "Truniger." On April 28, 2019, Truniger released files on the hacker forum Exploit that had been extracted from CityComp, a German IT services firm, following a ransomware attack. The post disclosed that the files were made public for free because CityComp had declined to pay the ransom. Although Truniger did not specify the attackers' identity or their affiliated group, the operation was attributed to the 'Snatch team' by German media. Subsequently, the Snatch team published 13 GB of data from an Italian insurance company on the Exploit forum, including sensitive information such as insurance checks, bank transfer details, and personal data of Italian citizens.[52]

Team Snatch was instrumental in popularizing the double extortion tactic, where attackers not only encrypt the victim's data but also threaten its public release. This extortion approach, as demonstrated by incidents like the Lehigh Valley Health Network data breaches, places victims in an exceedingly precarious position, enhancing the attackers' leverage. This evolution in ransomware strategy meant that incidents now often qualify as data breaches, potentially subjecting victims to legal obligations such as notifying affected individuals. Furthermore, it altered the interaction between ransomware operators and the media, with attackers increasingly exploiting public reporting to pressure their victims.

An incident on November 15, 2019, that underscores this shift, occurred when Lawrence Abrams, editor of the cybersecurity news site *BleepingComputer*, received an email from the "Maze Crew" while finishing his workday. This group is notorious for deceptive spam campaigns pretending to be a government agency and had previously targeted Abrams.[53] Back in May, he and a fellow security researcher had dissected Maze's code, uncovering a reference to *BleepingComputer*. Subsequently, Maze escalated their provocations by embedding Abrams' email address in malware deployed in a spate of attacks across Italy.[54] The situation intensified with the November email, transforming Abrams into a participant in Maze's operations. The message revealed that Maze had compromised Allied Universal, a major security services company based in Pittsburgh, boasting a workforce of 800.000:

> "I am writing to you because we have breached Allied Universal security firm (aus.com), downloaded data and executed Maze ransomware in their network.
> They were asked to pay ransom in order to get decryptor and be safe from data leakage, we have also told them that we would write to you about this situation if they dont pay us, because it is a shame for the security firm to get breached and ransomwared.
> We gave them time to think until this day, but it seems they abandoned payment process.
> I uploaded some files from their network as the data breach proofs. If they dont begin sending requested money until next Friday we will begin releasing on public everything that we have downloaded from their network before running Maze."

[46] The Economist, "Our Big Mac Index Shows How Burger Prices Are Changing," January 25, 2024, https://www.economist.com/big-mac-index

[47] Granger, "Fatboy Ransomware-as-a-Service Emerges on Russian-Language Forum."

[48] Translation from: Diana Granger, "Fatboy Ransomware-as-a-Service Emerges on Russian-Language Forum," *Recorded Future*, May 4, 2017, https://www.recordedfuture.com/blog/fatboy-ransomware-analysis

[49] AdvIntel, "Digital 'Pharmacusa' II: The 'GandCrab' Phenomenon," Internet Archive: WayBackMachine, January 26, 2023, https://web.archive.org/web/20230126230909/https://www.advintel.io/post/digital-pharmacusa-ii-the-gandcrab-phenomenon

[50] This argument was also presented by AdvIntel in their "Digital 'Pharmacusa' II: The 'GandCrab' Phenomenon" write-up.

[51] Brian Krebs, "Who's Behind the GandCrab Ransomware?" *Krebs on Security*, July 8, 2019, https://krebsonsecurity.com/2019/07/whos-behind-the-gandcrab-ransomware/

[52] AdvIntel, "Digital 'Pharmacusa' II: The 'GandCrab' Phenomenon," October 29, 2019, https://web.archive.org/web/20230126230909/https:/www.advintel.io/post/digital-pharmacusa-ii-the-gandcrab-phenomenon

[53] Lawrence Abrams, "Allied Universal Breached by Maze Ransomware, Stolen Data Leaked," *BleepingComputer*, November 21, 2019, https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/; Sophos, "Maze Ransomware: Extorting Victims for 1 Year and Counting," *Sophos News*, May 12, 2020, https://news.sophos.com/en-us/2020/05/12/maze-ransomware-1-year-counting/

[54] For the longer story see: Dudley and Golden, *The Ransomware Hunting Team*.

The email included a small sample of the purportedly stolen files to substantiate their claims. In the follow up emails, the Maze Crew explained they demanded 300 Bitcoins, then worth approximately 2.3 million USD, to decrypt all the files on Allied Universal's computer systems. They explained that the exfiltration of the files, and potential leak, was done to create further leverage to have the victim pay the ransom. Maze also threatened to start a spam campaign using Allied Universal's domain name and email certificates if payment was not made, introducing a new level of extortion tactics. This approach, termed "triple extortion," not only involves demanding a ransom for data decryption (single) and threatening data leakage (double) but also includes the threat of additional attacks if the ransom is not paid.

Following the creation of a leak site by Maze, this multi extortion method became a trend among ransomware groups, leading to the creation of leak sites, also known as "shaming blogs," by other groups.[55]

Overall, ransomware attacks became not just about encrypting data, but about stealing sensitive information before the encryption. This complicates the recovery process, as merely restoring data from backups does not address the potential release of stolen information. Ransomware groups leverage "leak sites" to exert pressure on victims through the threat of reputational damage and regulatory issues. This tactic forces victims to respond under pressure, potentially disrupting a measured recovery process.

7 Professionalization

Following the adoption of double and triple extortion tactics, there was a marked escalation in ransomware attacks globally.[56] This period also saw the professionalization of ransomware operations, exemplified by the rise of REvil, also known as Sodinokibi. Emerging in April 2019, REvil is often considered the successor to GandCrab, due to similarities in their codes and organizational structures.[57] This professionalization manifests in the greater planning and structured execution of attacks, featuring a clearer division of responsibilities within ransomware groups.[58] They also expanded their reach, targeting even larger and more secure entities and demanding increasingly high ransoms.

Since its foundation, REvil stood out for its adept use of the RaaS model. The person behind the moniker "UNKN" or "Unknown" spearheaded recruitment efforts through various underground forums in May 2019, seeking a small group of skilled affiliates. These recruitment posts promised an attractive profit-sharing model, starting at 60 percent and increasing to 70 percent following three successful operations. To enhance the legitimacy of these offers, UNKN placed a significant cryptocurrency deposit, initially around 130.000 USD, which was later increased to 1 million USD during further recruitment drives.[59] UNKN was pivotal not just in assembling a skilled team but also in shaping REvil's public image, engaging in interviews with media like *The Record* and YouTuber Russian OSINT, disclosing the group's expansion to around sixty affiliates.[60] In July 2021, UNKN mysteriously disappeared which led to "0_neday" taking over.[61]

---

[55] Magno Logan et al., "The State of Ransomware: 2020's Catch-22 - Security News," *Trend Micro IE*, February 3, 2021, https://www.trendmicro.com/vinfo/ie/security/news/cybercrime-and-digital-threats/the-state-of-ransomware-2020-s-catch-22

[56] Ani Petrosyan, "Global Number of Ransomware Attacks Q1 2020-Q4 2022," Statista, August 29, 2023, https://www.statista.com/statistics/1315826/ransomware-attacks-worldwide/; Rajeev Syal, "Ransomware Attacks in UK Have Doubled in a Year, Says GCHQ Boss," *The Guardian*, October 25, 2021, https://www.theguardian.com/uk-news/2021/oct/25/ransomware-attacks-in-uk-have-doubled-in-a-year-says-gchq-boss; John Sakellariadis also suggests that since 2019, there has been a professionalization of ransomware. He points out that the clearest sign of how ransomware has transformed cybercrime markets from this period is the rise of illicit access brokers and the marketplaces where they operate. See: John Sakellariadis, "Behind the Rise of Ransomware," *Atlantic Council*, August 2022, https://www.jstor.org/stable/resrep42765

[57] See McAfee Blog, part 1-4: McAfee Labs, "McAfee ATR Analyzes Sodinokibi Aka REvil Ransomware-as-a-Service - What The Code Tells Us," *McAfee Blog*, October 2, 2019, https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-what-the-code-tells-us/; John Fokker, "Dismantling a Prolific Cybercriminal Empire: REvil Arrests and Reemergence," Trellix, September 29, 2022, https://www.trellix.com/blogs/research/dismantling-a-prolific-cybercriminal-empire/

[58] You could also describe them as adopting a more corporate structure, with specialized roles such as dedicated HR or payroll managers being introduced.

[59] Brian Krebs, "Is 'REvil' the New GandCrab Ransomware?" *Krebs on Security*, July 15, 2019, https://krebsonsecurity.com/2019/07/is-revil-the-new-gandcrab-ransomware/

[60] Russian OSINT, "ЭЛИТНЫЕ ХАКЕРЫ REVIL/SODINOKIBI: $100 МИЛЛИОНОВ НА ШИФРОВАЛЬЩИКЕ?" Youtube, October 23, 2020, https://www.youtube.com/watch?v=ZyQCQ1VZp8s; Dmitry Smilyanets, "'I Scrounged through the Trash Heaps ... Now I'm a Millionaire:' An Interview with REvil's Unknown," *The Record*, March 16, 2021, https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown; Lawrence Abrams, "Another Ransomware Will Now Publish Victims' Data If Not Paid," *BleepingComputer*, December 12, 2019, https://www.bleepingcomputer.com/news/security/another-ransomware-will-now-publish-victims-data-if-not-paid/

[61] Jonathan Greig, "REvil Ransomware Operators Claim Group Is Ending Activity Again, Victim Leak Blog Now Offline," *ZDNET*, October 18, 2021, https://www.zdnet.com/article/revil-ransomware-operators-claim-group-is-ending-activity-again-happy-blog-now-offline/

After successfully breaching and encrypting the data of their targets, REvil would leave behind a ransom note, promptly alerting the victim to the encryption and directing them to purchase a decryption key to regain access. To create a sense of urgency, the note included a timer and a warning that the ransom amount would double once the timer expired.[62] Victims were directed to negotiate over REvil's Tor site, allowing direct communication with the group's representatives. To exert further pressure, REvil sometimes shared snippets of the stolen data during negotiations.[63] Aware that these discussions were publicly accessible, REvil offered the option for private communication as well.[64]

REvil's infamy surged in August 2019 following a significant supply-chain attack through a Managed Service Provider (MSP), affecting 23 Texas municipalities with a ransom demand of 2.5 million USD – one of the largest ransom payouts at the time. The group did not just rest on their laurels; they refined their tactics and expanded their reach, ensuring their affiliates had the latest in ransomware technology, targeting both Windows and Linux operating systems.[65] Following TeamSnatch's innovation, REvil quickly embraced the double extortion technique, using it by December to threaten the release of stolen data from the CyrusOne incident. [66] That same month, they also hit Travelex, netting a 2.3 million USD ransom.[67]

In March 2020, taking a cue from Maze's introduction of a leak site, REvil launched their own platform, dubbed the "Happy Blog." The blog was frequently updated with posts that sometimes mimicked official press releases. It later also introduced an eBay-style auction system for selling data belonging to non-compliant victims.[68] Their most high-profile exploitation of double extortion occurred in May 2020 with the theft of 756 GB of data from GSMLaw, a law firm whose clients included Donald Trump, Madonna, and Lady Gaga. REvil made headlines by auctioning off this high-profile data after GSMLaw declined to meet their demands.[69]

In 2020, REvil became the leading ransomware variant, focusing its attacks on organizations in North America and Europe, while notably avoiding CIS countries and Syria.[70] In one interview, UNKN also mentioned a particular interest in companies with cyber insurance, viewing them as more inclined to pay ransoms and even contemplating hacking insurance companies to identify prospective targets from their client lists.[71] Despite numerous instances of REvil engaging in re-extortion – demanding additional ransoms from victims who had already paid once, contrary to their promises of deleting the stolen data – this tactic seemingly did little to tarnish REvil's reputation, as many companies continued to meet their demands.[72]However, REvil's most impactful actions were still on the horizon. In May 2021, they targeted JBS Meatpacking, the largest meat supplier globally, disrupting its operations and eventually extracting an 11 million USD ransom to restore data.[73] The pinnacle of REvil's activities came in July 2021 with an attack on a Remote Access Software provider through a supply-chain exploit. They ex-

---

[62] Mathew J. Schwartz, "REvil's Ransomware Success Formula: Constant Innovation," *Bank Info Security*, July 2, 2021, https://www.bankinfosecurity.com/revils-ransomware-success-formula-constant-innovation-a-16976

[63] Lawrence Abrams, "Asteelflash Electronics Maker Hit by REvil Ransomware Attack," *BleepingComputer*, April 2, 2021, https://www.bleepingcomputer.com/news/security/asteelflash-electronics-maker-hit-by-revil-ransomware-attack/

[64] Lawrence Abrams, "JBS Paid $11 Million to REvil Ransomware, $22.5M First Demanded," *BleepingComputer*, June 10, 2021, https://www.bleepingcomputer.com/news/security/jbs-paid-11-million-to-revil-ransomware-225m-first-demanded/

[65] Fernando Martinez, "REvil's New Linux Version," *AT&T Cybersecurity*, July 1, 2021, https://cybersecurity.att.com/blogs/labs-research/revils-new-linux-version

[66] Abrams, "Another Ransomware Will Now Publish Victims' Data If Not Paid."

[67] Lawrence Abrams, "Sodinokibi Ransomware Says Travelex Will Pay, One Way or Another," *BleepingComputer*, January 9, 2020, https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-says-travelex-will-pay-one-way-or-another/; Ionut Ilascu, "Sodinokibi Ransomware Hits Travelex, Demands $3 Million," *BleepingComputer*, January 6, 2020, https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-hits-travelex-demands-3-million/; Anna Isaac et al., "Travelex Paid Hackers Multimillion-Dollar Ransom Before Hitting New Obstacles," *The Wall Street Journal*, April 9, 2020, https://web.archive.org/web/20221212140922/https://www.wsj.com/articles/travelex-paid-hackers-multimillion-dollar-ransom-before-hitting-new-obstacles-11586440800

[68] This was a clear departure from their previous practice of freely posting stolen data. UNKN also mentioned that he contemplated engaging in personal harassment of company executives as a means to coerce payment, though it is unclear whether this approach was ever pursued. Dimitry Smilyanets, "'I Scrounged through the Trash Heaps ... Now I'm a Millionaire,'" *The Record*, March 16, 2021, https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown

[69] On their shame site, REvil announced that – as GSM seemed to be unwilling to pay – each week it would auction off the data of one celebrity and after allegedly having successfully sold Trump's data, Madonna would be next. Ionut Ilascu, "REvil Ransomware Found Buyer for Trump Data, Now Targeting Madonna," *BleepingComputer*, May 18, 2020, https://www.bleepingcomputer.com/news/security/revil-ransomware-found-buyer-for-trump-data-now-targeting-madonna/

[70] Nomios Group, "What Is REvil Ransomware?", accessed on May 5, 2024, https://www.nomios.com/resources/what-is-revil-ransomware/; Jessica Saavedra-Morales, "McAfee ATR Analyzes Sodinokibi Aka REvil Ransomware-as-a-Service - Crescendo," *McAfee Blog*, October 21, 2019, https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-crescendo/

[71] Dimitry Smilyanets, "'I Scrounged through the Trash Heaps ... Now I'm a Millionaire,'" *The Record*, March 16, 2021, https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown

[72] Coveware: Ransomware Recovery First Responders, "Q3 Ransomware Demands Rise: Maze Sunsets & Ryuk Returns," November 4, 2020, https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

[73] BBC News, "JBS: Cyber-Attack Hits World's Largest Meat Supplier," June 2, 2021, https://www.bbc.com/news/world-us-canada-57318965; Lawrence Abrams, "JBS Paid $11 Million to REvil Ransomware, $22.5M First Demanded," *BleepingComputer*, June 10, 2021, https://www.bleepingcomputer.com/news/security/jbs-paid-11-million-to-revil-ransomware-225m-first-demanded/

ploited a zero-day vulnerability in Kaseya's Virtual Systems Administrator (VSA) software, spreading ransomware via a fake update. This attack affected over 1.500 companies across the world, with REvil demanding an extraordinary 70 million USD for a universal decryption key, showcasing the extensive reach of their operations.[74]

8 Ransom War Groups

Ransomware groups have evolved significantly over recent years. Groups like REvil, which are at the forefront of this disturbing development in the criminal ecosystem, can best be described as *ransom war groups* rather than simple ransomware groups.[75] These groups have shown both the capability and willingness to orchestrate operations against significant targets driven by the prospect of financial gain. This not only includes major supply-chain attacks, such as REvil's ransomware attack on 1.500 companies through Kaseya. Ransomware attacks on national government institutions are also prevalent, with examples like Conti's disruptive activities in Costa Rica as well as Cuba ransomware group's attack on Montenegro's Department for Public Relations in August 2022, Quantum's attack on the Dominican Agrarian Institute the same month, and RansomHouse's attack on Colombian government ministries in September 2023.[76] Ransom war groups distinguish themselves by their relatively high level of organization and operational planning. Additionally, they cultivate a distinct brand identity and reputation.

Ransom war groups often deliberately execute operations that directly threaten human lives and critical infrastructure, thereby heightening the consequences of non-payment and enhancing their coercive leverage. A stark illustration of this tactic was the ransomware assault by the Russian gang Qilin on prominent London hospitals in June 2024. The attack led King's College and Guy's and St Thomas' trusts – two major acute hospital trusts in London – to postpone 832 surgeries, including critical procedures such as cancer treatments, organ transplants, and heart surgeries, over the course of a week. [77]

At other times, the drive for maximizing profit has led these groups to inadvertently impact human or national security. Ransom war groups often target organizations whose compromise can have broader security implications, which the attackers may not fully appreciate or even wish to avoid, lest it draw significant governmental attention. A contentious example of this is Darkside's ransomware attack on Colonial Pipeline, a company responsible for nearly half the fuel supply for the US East Coast. The breach of Colonial Pipeline's IT systems prompted the company to cease its operations out of concern the attack could spread further. This action triggered a regional emergency declaration by the Federal Motor Carrier Safety Administration on May 9, leading to panic buying and significant fuel shortages across states like North Carolina and Georgia. Subsequently, on May 9, the Federal Motor Carrier Safety Administration issued a regional emergency declaration for eighteen states. It led to panic buying and petrol shortages in several states, such as North Carolina and Georgia. In response, the Biden Administration explored alternative transportation methods for fuel via trucks, trains, and ships. Furthermore, on May 12, President Biden enacted an executive order to implement new cybersecurity standards for software sold to

[74] Unlike in most other cases at the time, REvil refrained from exfiltrating data before encrypting the victims' data. The Ransomware Files Podcast, "The Ransomware Files Podcast, Episode 6: Kaseya and REvil," Youtube, April 8, 2022, https://www.youtube.com/watch?v=dO8hNhi9WmM; As it was launched just before a holiday weekend, it did not have as much impact in Europe. Thomas Kuhn, "Kaseya-Attacke: Wie der Deutsche Feierabend der Kaseya-Attacke Zum Verhängnis Wurde," *WirtschaftsWoche*, July 9, 2021, https://www.wiwo.de/technologie/digitale-welt/kaseya-attacke-wie-der-deutsche-feierabend-der-kaseya-attacke-zum-verhaengnis-wurde/27404374.html

[75] The term has earlier references to significant ransomware incidents. For an overview see Will Thomas' talk at Sleuthcon: Will Thomas, "Xakep, Repa, Probiv, Spy," Sleuthon, May 24, 2024; Also see: Nissim Ben Saadon, "Ransom-War Escalation: The New Frontline in Cyber Warfare." Cyber Defence Magazine, February 22, 2024, https://www.cyberdefensemagazine.com/ransom-war-escalation-the-new-frontline-in-cyber-warfare; Robin Pomeroy, host. "Ransomware and 'Ransom-War': Why We All Need to Be Ready for Cyberattacks." Radio Davos, World Economic Forum, April 1, 2022, https://www.weforum.org/podcasts/radio-davos/episodes/cybersecurity/; Natto Team. "Ransom-War: Russian Extortion Operations as Hybrid Warfare, Part One." Natto Thoughts. May 1, 2024; https://nattothoughts.substack.com/p/ransom-war-russian-extortion-operations; James McQuiggan. "Ransomware, Ransom-War and Ran-some-where: What We Can Learn When the Hackers Get Hacked." KnowBe4, 2022, https://info.knowbe4.com/ransomware-ransom-war

[76] Sri Lanka also suffered from a significant ransomware attack but did not disclose which group was behind the attack. On Cuba's attack against Montenegro: *Reuters*, "Montenegro blames criminal gang for cyber attacks on government," September 1, 2022, https://www.reuters.com/world/europe/montenegro-blames-criminal-gang-cyber-attacks-government-2022-08-31/; UK Parliament, "Written evidence submitted by BAE Systems," December 1, 2022, https://committees.parliament.uk/written-evidence/114375/pdf/; On Quantum's attack against the Dominican Republic: Jonathan Greig, "Dominican Republic refuses to pay ransom after attack on agrarian institute," *The Record*, August 26, 2022, https://therecord.media/dominican-republic-refuses-to-pay-ransom-after-attack-on-agrarian-institute; On Ransomhouse: Jonathan Greig, "Several Colombian Government Ministries Hampered by Ransomware Attack," *The Record*, September 15, 2023, https://therecord.media/colombia-government-ministries-cyberattack

[77] BBC, "Critical incident over London hospitals' cyber-attack," June 4, 2024, https://www.bbc.com/news/articles/c288n8rkpvno. Later figures suggest a much higher number of medical procedures that had to be postponed, with often extremely harmful consequences to patients: Connor Jones, "Cancer patient forced to make terrible decision after Qilin attack on London hospitals," *The Register*, July 5, 2024, https://www.theregister.com/2024/07/05/qilin_impacts_patient/

the federal government and to set up an incident review board to extract lessons from major hacking incidents.[78] Yet, Darkside later stated that it had not intended to precipitate such severe societal repercussions and would monitor its targets more closely in the future. The sincerity of such statements is of course debatable given the group's track record and previous PR stunts.

9 Conclusion

Popp was an early pioneer of ransomware, but significant differences separate his exploits from those of modern-day ransomware groups. Unlike Popp, modern ransomware groups have successfully found ways to monetize their malicious activities. This achievement can be attributed to various innovations, including improved encryption methods and streamlined payment processes, among others. Today's ransomware groups operate with a well-defined modus operandi, thriving within a well-funded and highly professionalized criminal ecosystem, characterized by increased specialization. Ransomware groups have evolved into recognized brands, utilizing their established reputation to engage with the internal criminal sector, victims, and the general public.

This shift in the ransomware landscape calls for more focused research and academic engagement to better understand the organizational dynamics of these groups and their impact on security. By deepening our understanding of how these criminal organizations function and interact with their environment, we can develop more effective policy responses to counter the growing threat they pose. This approach will be essential in addressing the evolving challenges of ransomware on both a national and global scale.

In *Ransom War: How Cyber Crime Became a Threat to National Security*, Max Smeets pursues three key objectives. First, he introduces the MOB framework to systematically deepen our understanding of ransomware by analyzing its i) modus operandi, ii) organizational structures, iii) and branding strategies. Second, he applies this framework to the Conti ransomware group, offering an in-depth case study that sheds light on broader cybercrime patterns. Lastly, he provides policymakers with actionable insights, enabling them to devise more effective strategies to combat ransomware.

[78] Colonial Pipeline, "Media Statement Updated: Colonial Pipeline System Disruption," Press Release, May 8, 2021, https://web.archive.org/web/20210508173736/https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption; Aaron Gregg, "Colonial Pipeline was shut down with worst-case scenario in mind, executives say," *Washington Post*, June 9, 2021, https://www.washingtonpost.com/business/2021/06/09/colonial-pipeline-mandiant-house-hearing/; Federal Motor Carrier Safety Administration, "Regional Emergency Declaration under CFR § 390.23," May 9, 2021, https://www.fmcsa.dot.gov/sites/fmcsa.dot.gov/files/2021-05/ESC-SSC-WSC%20-%20Regional%20Emergency%20Declaration%202021-002%20-%2005-09-2021.pdf;

About the Author

Dr. Max Smeets is a Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich and Co-Director of the European Cyber Conflict Research Initiative and Cyber Conflict Research Incubator. He is the author of 'No Shortcuts: Why States Struggle to Develop a Military Cyber- Force' (Oxford University Press & Hurst Publishers, 2022) and co-editor of 'Deter, Disrupt or Deceive? Assessing Cyber Conflict as an Intelligence Contest' (Georgetown University Press, 2023) and 'Cyberspace and Instability' (Edinburgh University Press, 2023).

Max is an affiliate at Stanford University's Center for International Security and Cooperation (CISAC) and an associate fellow at Royal United Services Institute (RUSI). He also lectures on cyber warfare and defense as part of the Senior Officer course at the NATO Defense College in Rome.

He recently co-founded Binding Hook, a new media outlet on technology and security part of ECCRI.

He was previously a postdoctoral fellow and lecturer at Stanford University CISAC and a College Lecturer at Keble College, University of Oxford. He has also held research and fellowship positions at New America, Columbia University SIPA, Sciences Po CERI, and NATO CCD COE. Before his academic career, Max worked in finance in London and Amsterdam.

Max received a BA in Economics, Politics and Statistics summa cum laude from University College Roosevelt, Utrecht University and an M.Phil (Brasenose College) and DPhil (St. John's College) in International Relations from the University of Oxford.

CSS
ETH Zürich

The **Center for Security Studies (CSS)** at ETH Zürich is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.