Q2 2023 Edition

SPONSORED BY:

CONCEAL

WHO'S WHO IN RANSOMWARE: 2023 REPORT

THE MOST ACTIVE RANSOMWARE GANGS AND THEIR VICTIMS

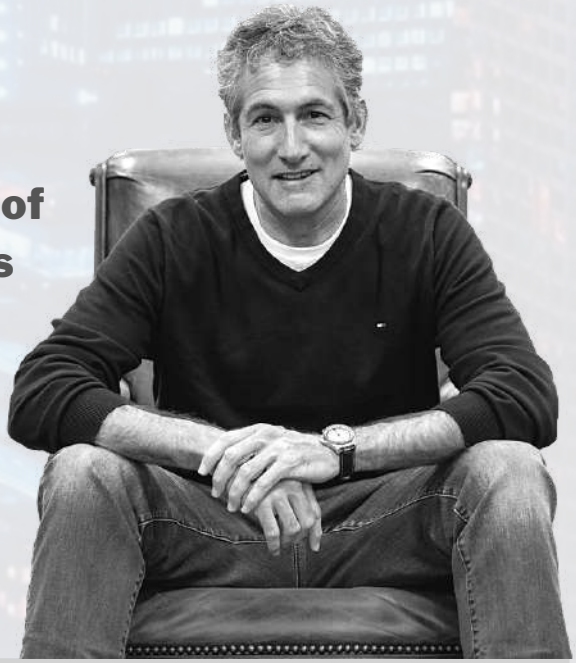
CYBERSECURITY VENTURES

WHO'S WHO IN RANSOMWARE REPORT

INTRODUCTION

Chief information security officers and cybersecurity teams are devoting more time than ever protecting against ransomware.

Steve Morgan, founder of Cybersecurity Ventures



Cybersecurity Ventures predicts ransomware will attack a business, consumer, or device every 2 seconds by 2031. Our goal with this report is to provide a window into the organized gangs who are planning and executing the attacks. Knowledge is power in the war against ransomware criminals.

– Steve Morgan, founder of Cybersecurity Ventures and Editor-in-Chief at Cybercrime Magazine

WHO'S WHO IN RANSOMWARE REPORT

TABLE OF CONTENTS

WHAT IS RANSOMWARE?

Ransomware is a malware variant designed to deny a user access to their files or systems and is roughly separated into crypto and locker types – although many ransomware families today combine these capabilities, and more.

Once ransomware has successfully infected a target machine or network, its operators attempt to extort their victims, whether individuals or organizations. They will use the lure of a decryption key (which may or may not work) to pressure the target into paying.

Ransomware may be able to move laterally across a network, propagate to connected PCs or storage drives, and use different levels of encryption. Furthermore, ransomware families make use of different programming languages ranging from C++ to Go.

Well-known ransomware variants include WannaCry, CryptoLocker, Conti, Evil Corp, Hive, Grief Group, and Lace Tempest.

RANSOM DEMANDS

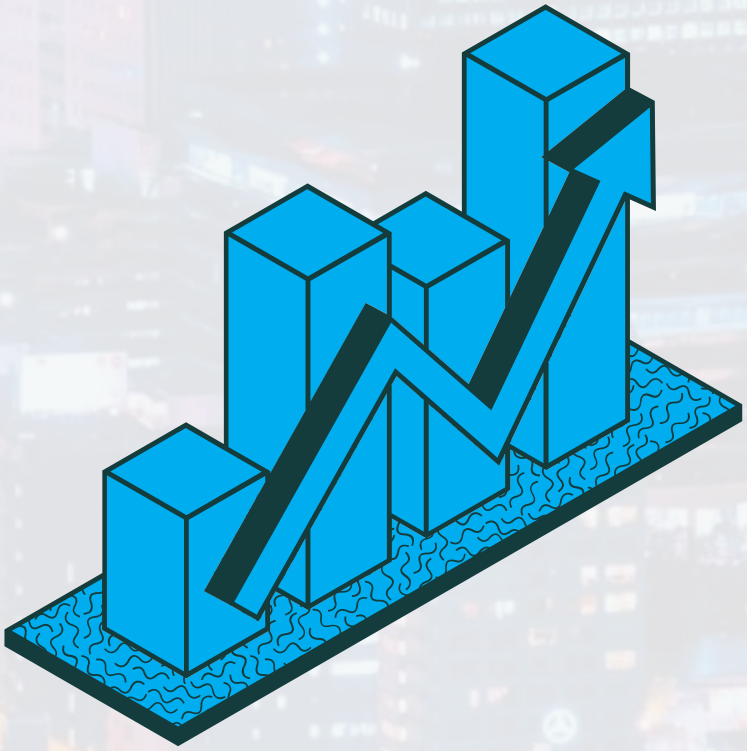
Ransomware gangs are, in almost every case, financially motivated. These cybercriminals will stop at nothing to be paid – whether this means locking up your personal information or grinding the operations of a Fortune 500 company to a halt.

Victims will be directed to websites in the Deep Web or secure chats to make a payment or negotiate a ransom. To disguise their tracks, ransom demands are made in cryptocurrency, most often Bitcoin (BTC), although other virtual coins including Ethereum (ETH) may occasionally make an appearance.

To date, the largest known ransomware payout was made by CNA Financial, a U.S. insurance company. Reports suggest the firm paid $40 million in an attempt to regain access to its systems following an attack by a ransomware group. Colonial Pipeline paid a $5 million ransom to cybercriminals in 2021. There have been other ransoms paid in the millions of dollars, and a mulititude in the five to six figure range.

RANSOM DEMANDS

There were 459 major business-related ransomware incidents in Mar. 2023 alone, a 91 percent month-on-month increase.



Ransom demands frequently reach millions of dollars, with many others falling within the range of five to six figures. If victims refuse, they may find themselves publicly “named and shamed” on leak sites and their confidential information may be publicly leaked.

GLOBAL RANSOMWARE COSTS

Ransomware is now synonymous with a thriving cybercrime economy.

While ransomware infections were once considered a consequence of visiting illicit websites or downloading illegal, cracked software, it is now a weapon of choice for cybercriminals indiscriminately attacking SMBs and Fortune 500 organizations alike.

The reasons ransomware exists are for blackmail and financial extortion. Despite CISOs and cybersecurity teams pouring resources into ransomware protection and law enforcement worldwide cracking down on the lucrative, illegal industry, ransomware showed no signs of stopping in Q2 2023.

Ransomware gangs are relentlessly jockeying for position as the most dangerous threats to network defenders.

The US Financial Crimes Enforcement Network (FinCEN) says that ransomware still poses a

GLOBAL RANSOMWARE COSTS

significant threat to U.S. businesses and the public. For example, suspicious transactions suspected of being tied to ransomware and reported under the Bank Secrecy Act reached $1.2 billion in 2021.

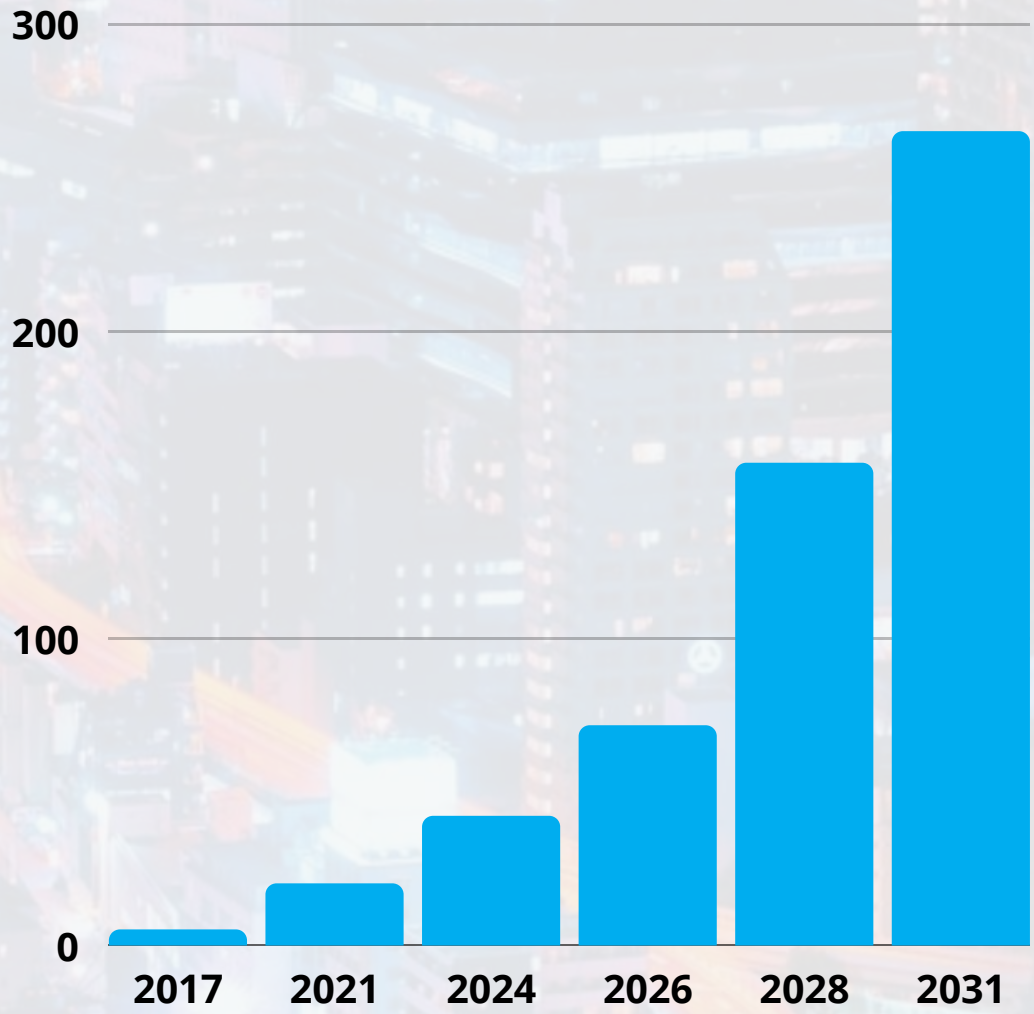
Cybersecurity Ventures predicts that by 2031, ransomware will cost its victims approximately $265 billion, based on a 30 percent year-over-year growth over the next decade.

The costs include ransom payments, damage and destruction of data, lost productivity, theft of intellectual property, theft of personal and financial data, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

A ransomware attack is predicted to occur against consumers or businesses every two seconds by 2031, up from every 11 seconds in 2021.

GLOBAL RANSOMWARE COSTS

Ransomware is predicted to cost the world $265 billion annually by 2031, up from $5 billion in 2017.



OPERATION LANDSCAPE

Ransomware operations can take many forms. For example, unsophisticated gangs might rely on phishing and spam, whereas other more advanced gangs may take the time to perform reconnaissance first and select their targets more carefully.

Ransomware groups and services also operate differently. In some cases, groups buy commercially-available ransomware licenses, known as Ransomware-as-a-Service (RaaS), whereas others may develop their custom variants and guard them jealously.

What should be noted is that the ransomware economy and landscape is now more akin to a corporation than the Wild West.

Ransomware gangs may hire professionals to perform different roles, provide customer service, collaborate with other cybercriminals, or take “commissions’ when a client using their ransomware strain successfully extorts payment from a victim.

OPERATION LANDSCAPE

Many ransomware gangs specifically target what is known as “Big Game.” Big Game are high-profile, high-value enterprise firms with large annual revenue streams – as well as a lot to lose if they experience downtime.

The motive behind targeting Big Game is the possibility of higher payouts, often reaching millions of dollars. Recent Big Game targets include Dish Network, PharMerica, Capita, and ABB.

GEOPOLITICS

If you consider ransomware a business – albeit a criminal enterprise – politics, law, and the economy will impact the industry.

Ransomware operators, especially state-sponsored ones, do not operate in a vacuum and may launch politically-motivated attacks. For example, suspected Russian hackers attacked global communications firm Viasat, with their primary target being the Ukrainian military, an hour before the invasion began.

A local government's attitude to cybercrime can also change its relationship with other political factions.

For many years, the Kremlin has made superficial promises to crack down on cybercrime. This failure to rein in cybercrime has global consequences. Before the invasion of Ukraine, for example, Russia was not invited to a White House meeting with global leaders on how to disrupt ransomware operations, and other countries have since expanded threat intelligence-sharing deals.

GEOPOLITICS

In 2022, the U.S. and Canada renewed the Cross-Border Crime Forum to improve reporting concerning ransomware impacting cross-border critical infrastructure, and representatives of the U.S. and EU met to collaborate in fighting ransomware, now described as “a global problem that requires cooperation on a worldwide level.“

The U.S., U.K., and EU are critics of Russia, China, and North Korean for abetting ransomware attacks originating from their respective countries. Google’s Threat Analysis Group says that Ukraine is the main focus of Russian threat actors in 2023.

TACTICS

SPAM & PHISHING: The most common way that ransomware spreads is through mass, generic spam emails and social media links, leading to the download of malicious attachments or drive-by downloads. However, attacks may be more likely to succeed when social engineering is involved.

BRUTE FORCE ATTACKS: Automated brute force attacks are used to try and obtain user account credentials and gain entry into a target network.

INITIAL ACCESS BROKERS: IABs are traders in the Dark Web who sell initial access points to companies, including stolen credentials or working RDP tunnels. By purchasing initial access, ransomware gangs can avoid a time-consuming stage of the attack chain and go straight into network reconnaissance or infection.

RECONNAISSANCE, SOCIAL ENGINEERING: Sophisticated ransomware groups will often perform surveillance on a target to learn about them, and business connections, friends, families, or suppliers.

TACTICS

They may also conduct Open Source Intelligence (OSINT) activities to gather public knowledge about their targets. Armed with this information, attackers may masquerade as trusted contacts to lure their victims into unwittingly executing ransomware.

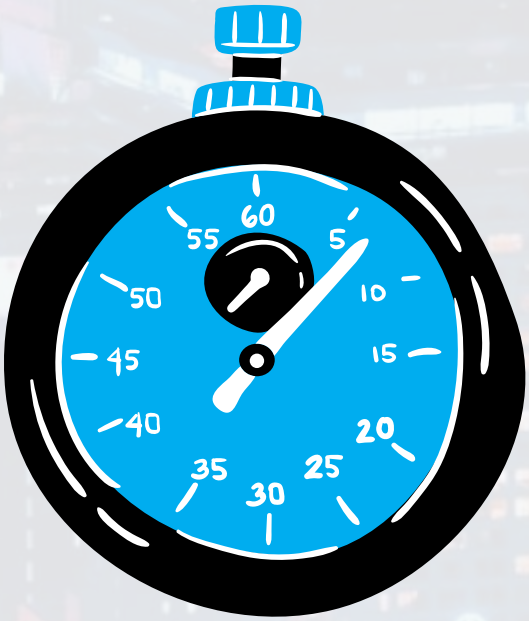
REMOTE DESKTOP PROTOCOL: Exploitation of RDP is a common way for ransomware operators to intrude on your network. RDP is exploitable through software vulnerabilities and hijacking user accounts, logged in through off-site locations.

EXPLOIT KITS: Exploit kits, such as Hunter, RIG, and Blackhole may all bundle ransomware into a malicious package, combining it with software exploits to gain access to a vulnerable computer.

INSIDERS: If a cyber gang can find a disgruntled employee, this becomes an insider threat. The employee may be offered cash or a percentage of a ransom to deploy a malicious payload from inside a network or 'fall' for a phishing attempt.

TACTICS

DOUBLE EXTORTION: Double extortion consists of two tactics to extort payment. Confidential data is stolen prior to encryption, and then cybercriminals threaten to publish this information online unless they are paid.



LEAK SITES: Leak sites are hosted in both the clear and Deep web. These websites act as name-and-shame portals for victims of ransomware, in which they are threatened with their data being published if a ransomware payment is not made by a specific date or time.

RANSOMWARE GANGS

As some ransomware gangs form and others close – or rebrand – the ones to watch constantly evolves.

AKIRA: Launched in Mar. 2023, Akira is a new entrant focused on attacking organizations in finance, property, education, manufacturing, and more.

ALPHV/BLACKCAT: The RaaS gang was first detected in late 2021. Affiliates have adopted the BlackCat ransomware in droves and the group is thought to have ties with now-defunct DarkSide and BlackMatter. In 2023 the group claimed it had attacked an Irish university and Western Digital.

AVOSLOCKER: AvosLocker has peddled its wares since 2021. The RaaS gang has launched high-profile attacks on the healthcare sector.

BABUK: Babuk's source code leaked in 2021. Smaller actors, including Ransom House and Play, are using the code to build ESXi lockers.

RANSOMWARE GANGS

BIANLIAN: BianLian uses a Go-based ransomware and infrastructure that first appeared in Dec. 2021. Researchers have taken note of this relatively new threat due to high speeds of encryption. While a free decryptor has been released, in Mar. 2023, researchers noted a pivot in tactics to rely purely on data theft and extortion to generate income.

BLACK BASTA: First discovered in Apr. 2022, Black Basta is a new entry that has claimed at least 50 organizations as victims. Some evidence points toward a Russian origin. The ransomware group reportedly claimed Swiss multinational company ABB as a victim in May 2023.

BLACKBYTE: BlackByte has claimed victims worldwide, ranging from Mexico to Vietnam. The RaaS group is a Big Game hunter and runs an interesting blackmail model: victims can pay smaller amounts to delay publishing of stolen data, and higher sums for downloads or deletion. Recently, BlackByte has adopted double-extortion methods.

RANSOMWARE GANGS

BL00DY: The FBI and CISA issued a joint warning in May, urging organizations to be on the alert against Bl00dy, a ransomware gang utilizing PaperCut vulnerabilities to attack the education sector.

CL0P: A RaaS service and prolific threat group, CLOP has extorted an estimated $500+ million from victim organizations. While arrests have been made, the RaaS service is alive and well.

CONTI/WIZARD SPIDER: When Russia invaded Ukraine, Conti pledged its support to Russian President Vladimir Putin. A disgruntled researcher responded by breaking into the gang's systems and leaking their files, leading to Conti's retirement. Researchers suspect members moved to BlackCat, AvosLocker, Hive, and HelloKitty.

CUBA: Since Dec. 2021, the Cuba ransomware outfit's number of U.S. victims has doubled with increased payouts. Links are suspected with RomCom RAT and Industrial Spy ransomware.

RANSOMWARE GANGS

DARKANGELS: Potentially a rebrand of Babuk, DarkAngels emerged in 2022 and conducts highly-targeted attacks.

DARKBIT: DarkBit is a new entrant to the list. The group attacked one of Israel's leading research universities in 2023. DarkBit appears to have a political ax to grind, considering its ransom note was laden with anti-Israel messaging.

DARKSIDE: DarkSide, believed to be in Eastern Europe, caused fuel panic-buying in the U.S. in 2021 after hitting Colonial Pipeline. The RaaS service is believed to count Brenntag and Toshiba Tec among its victims. The group said it was shutting down in 2021, but many ransomware gangs retire a brand, regroup, and then reemerge with a new name.

DAIXIN TEAM: Daixin Team was allegedly responsible for a Nov. 2022 attack on AirAsia, resulting in the leak of passenger and staff data, and they attacked B&G Foods this year.

RANSOMWARE GANGS

DEADBOLT: Active since Jan. 2023, the Deadbolt group demands Bitcoin following the encryption of NAS drives. In Oct. 2022, Dutch police tricked the group into handing over 150 decryption keys.

DOPPELPAYMER: A rebrand of BitPaymer, DoppelPaymer strikes organizations in healthcare, education, and emergency services. After disrupting a German hospital, prosecutors attempted to pursue the hackers with negligent homicide, but the case was eventually dropped due to a lack of evidence. It is thought that the gang has rebranded to Grief Group.

EVIL CORP: Known for attacking CNA Financial, Evil Corp is believed to be in Russia. In 2022, Microsoft linked the use of the Raspberry Robin worm and FakeUpdates malware in attacks to the gang.

FIN7/SANGRIA TEMPEST: FIN7 is a notorious Russian hacking group that emerged in May. Having previously deployed REvil and Maze ransomware, the gang now uses Cl0p ransomware in targeted attacks.

RANSOMWARE GANGS

GRIEF GROUP: Suspected of being a rebrand of DoppelPaymer and also known as PayOrGrief, the gang managed to claim over $10 million in ransom payments mere months after launch. Rebrand aside, Europol has raided the homes of individuals suspected of being the masterminds of DoppelPaymer attacks.

HARDBIT: First observed in Oct. 2022, HardBit takes negotiation to the next level. The gang will try and convince its victims to reveal cyber insurance policy information so a ransom demand can be made within payout parameters.

HELLOKITTY: HelloKitty/FiveHands, likely Ukrainian and with ties to Russian cybercriminals, is best known for stealing information belonging to game developer CD Projekt Red. HelloKitty will launch DDoS attacks against victims who refuse to pay.

HIVE: Hive has operated a RaaS service since at least 2021. Hive actors have victimized at least 1,500

RANSOMWARE GANGS

companies worldwide, receiving at least $100 million in payments. In 2023, the U.S. DoJ announced the FBI's infiltration of Hive's network, with its infrastructure dismantled and over 300 decryption keys released to victims.

INDUSTRIAL SPY: Industrial Spy emerged in Apr. 2022 and will either steal data for extortion alone or conduct theft and deploy ransomware.

LAPSUS$: LAPSUS$ was an infamous group that conducted a double-extortion hacking spree, claiming high-profile victims including Microsoft, Nvidia, and Okta. While no longer active, a 16-year-old from the UK who still lived with his mother is suspected of being a leader.

LOCKBIT: According to Digital Shadows, LockBit infection rates outstrip every other group by a substantial margin, accounting for over 30 percent of all recorded infections. LockBit took credit for an attack on the U.K.'s Royal Mail service in Jan. 2023.

RANSOMWARE GANGS

Although Darktrace denies these claims, LockBit boasts of infiltrating the cybersecurity firm's systems. LockBit also targets macOS devices.

MEDUSA: Medusa ramped up its activity this year with a rash of attacks, million-dollar demands, and the launch of a leak site. An Australian cancer treatment center received a $100,000 demand in May 2023. Medusa also leaked what is allegedly Microsoft source code.

MONEY MESSAGE: Money Message claimed responsibility for the breach and theft of source code from Micro-Star International (MSI), with screenshots of stolen data later posted on a leak site.

MORTALKOMBAT: MortalKombat is a new ransomware variant spread through cryptocurrency-themed phishing emails. As the ransomware was only observed in early 2023, little is currently known about the threat actors behind it beyond that the majority of victims are based in the U.S.

RANSOMWARE GANGS

NETWALKER: In 2020, Netwalker attacked the University of California SF. To salvage its research, the educational institution paid the group $1.14 million. A Canadian national and affiliate of the group was recently sentenced to 20 years behind bars.

NEVADA: In Feb. 2023, the sudden emergence of a new ransomware gang, dubbed Nevada, captured the attention of researchers. The group reportedly attempted to compromise roughly 5,000 systems belonging to organizations ranging from shipping to construction firms.

NOKOYAWA: Nokoyawa is relatively new, sharing code with another ransomware family known as Karma, and is still being investigated by researchers. The group is suspected of a link with Hive, which hit the headlines in 2021 after breaching approximately 400 organizations. Cybercriminals exploited a Microsoft Windows zero-day vulnerability to deploy Nokoyawa payloads prior to being patched. Many of its targets are in South America, mainly in Argentina.

RANSOMWARE GANGS

ONYX: Onyx operators focus on the U.S. This group conducts double-extortion attacks and may destroy data rather than encrypt it. Guatemala's Foreign Ministry was added to the Onyx leak site's victim list in 2022.

PANDORA: Pandora, a suspected rebrand of ROOK, has targeted high-profile organizations including automotive giant Denso Corp in 2022.

PLAY: Launched in Jun. 2022, Play is ransomware linked to attacks against Argentina's Judiciary of Córdoba and A10 Networks. The gang continues to enhance its weapon portfolio, having recently introduced two new custom tools in .NET.

RA GROUP: RA Group is using leaked Babuk source code to compromise organizations in the U.S. and South Korea. The new gang, in operation since roughly Apr. 2023, has claimed victims in manufacturing, wealth management, insurance, and pharmaceuticals – at the least.

RANSOMWARE GANGS

RAGNAR LOCKER: Ragnar Locker, both malware and a group itself, has been on the FBI watchlist since 2020. The group has attacked organizations in industries including energy, infrastructure, and financial services – as well as a misplaced attack against Dutch police.

RANSOMEXX: RansomEXX appeared in 2018 under the name Defray777 and remains active today. The RaaS service has links to the Gold Dupont group. According to Trend Micro, the ransomware marked the first time a major Windows strain expanded to Linux. A data leak post made by the group claimed Ferrari among its victims in Mar. 2023.

ROYAL: First spotted in 2022, Royal appears to focus on the healthcare sector, demanding millions of dollars in blackmail payments following successful attacks. Royal seems to be a private criminal gang rather than a RaaS service. Royal caused significant damage to government systems belonging to the City of Dallas.

RANSOMWARE GANGS

RYUK: Emerging in 2018, Ryuk ransomware has been connected to Emotet and Trickbot botnet operators. This ransomware was employed before the group behind Ryuk campaigns, Wizard Spider, switched to Conti. In February, a Russian national, extradicted to the U.S. in 2022, pleaded guilty for laundering the proceeds of Ryuk ransom payments.

SANDWORM: Russian-backed Sandworm has launched RansomBoggs novel ransomware against Ukrainian organizations. Also known as BlackEnergy, this group is not specifically focused on ransomware; rather, it is known to also use wiper malware against its targets. New, destructive features were added to Sandworm malware in early 2023.

SNATCH: Active for many years, Snatch ransomware forces a compromised PC into reboot mode before encryption occurs. Attacks recorded include an incident involving the Californian city Modesto and a Wisconsin school.

RANSOMWARE GANGS

SODINOKIB/REVIL: Sodinokibi, or REvil, is a Russian-speaking group focusing on high-value targets. Past victims include Kaseya. In Mar. 2022, the U.S. DoJ charged an alleged group member for participating in the attack. Recent analysis suggests REvil may, once again, be under active development.

THANOS: The Thanos RaaS service and 'create your own' ransomware software service was a one-man-band created and licensed by a resident of Venezuela. An FBI investigation led to his arrest.

VICE SOCIETY: Joining the scene in 2021, Vice Society is a group that employs double-extortion tactics against victim organizations. However, the group does not develop its own malware; instead, it prefers to rely on commercial malware. This year, Vice Society has focused on attacking British schools and manufacturing companies.

YASHMA/CHAOS: Yashma is potentially a rebrand of Chaos, although the development family tree is

RANSOMWARE GANGS

unclear. Researchers consider this ransomware strain – and its users, the Onyx group – dangerous considering its flexibility. U.S. emergency services are among its victims.

YANLUOWANG: The Yanluowang ransomware gang was linked to a confirmed attack against Cisco in May 2022. Yanluowang added the tech giant to its leak site, claiming the theft of 2.75GB in stolen data.

WANNACRY: Wannacry is one of the most well-known and devastating ransomware attacks to date. In 2017, the ransomware attack, believed to be the work of North Korea, locked hundreds of thousands of PCs worldwide in a matter of hours.

ZEPPELIN: Zeppelin, a derivative of the Delphi-based Vega malware family, is a RaaS service known to have targeted enterprise companies, healthcare, and medical organizations from 2019 until today.

RANSOMWARE PROTECTION

There are many ways to protect yourself and your organization against ransomware, but for many businesses, it's not a case of if, but rather when, a cyberattack or breach occurs.

However, there are practices to increase security hygiene, including:

- Keeping operating systems and software up-to-date
- Analyzing the risk of new vulnerabilities and patching promptly
- Being aware of, and training to recognize phishing and social engineering attempts
- Avoiding suspicious websites and implementing firewalls
- Implementing zero-trust policies in user management
- Maintaining regular, offline backups
- Creating an incident response plan considering damage limitation, forensics, and legal aspects

RANSOMWARE RESOURCES

The official U.S. Cybersecurity & Infrastructure Agency website, CISA.gov, provides an in-depth guide for business leaders and responders, which can be accessed here. A key thing to remember is that even if you pay a ransom, there is no guarantee that your systems will be restored or your files will be returned.

StopRansomware.gov is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively.

Click here to report a cyber incident to CISA

Click here to report a ransomware incident to the FBI

The Mitre Ransomware Resource Center helps healthcare organizations become more resilient to threats from ransomware.

Cybercrime Magazine provides a feed covering the latest ransomware incidents.

WHO'S WHO IN RANSOMWARE REPORT

SPONSORED BY CONCEAL

“Ransomware attacks are coming, and companies of all sizes need to be prepared,” says Gordon Lawson, CEO at Conceal.

Gordon Lawson, CEO
Conceal

“Ransomware has evolved. On top of encrypting data that can’t be accessed without a stiff payment, ransomware gangs now routinely threaten to publish sensitive data — sometimes in searchable form. The more sophisticated gangs routinely scan corporate networks to find the data that will give them the most leverage when demanding ransom money. Meanwhile, beginners who can barely code can easily buy all the software they need to get into the game."

WHO'S WHO IN RANSOMWARE REPORT

ABOUT CONCEAL

Conceal is a fast-growing cybersecurity company that offers innovative technology solutions to our customers, globally. Each team member reflects our company's main goal: to protect the world from ever-growing cyber crimes.

Conceal provides a capability that protects people and critical assets against the most advanced threat actors in the world. We are fundamentally changing the approach to cybersecurity by creating a platform where security practitioners can see the latest threat vectors and implement enterprise-wide solutions that comprehensively protect their organization.

With our Conceal platform, we take those core capabilities and evolve them into a commercially available product that incorporates intelligence-grade, Zero Trust technology to protect global companies — of all sizes — from malware and ransomware.

To learn more, visit https://conceal.io

WHO'S WHO IN RANSOMWARE REPORT

WHO'S WHO IN RANSOMWARE Q2 2023 REPORT is written by Charlie Osborne, Editor-at-Large for Cybercrime Magazine. Steve Morgan, founder of Cybersecurity Ventures contributed.

Cybersecurity Ventures
83 Main Street, 2nd Flr., Northport, N.Y. 11768
info@cybersecurityventures.com