PRICE

2X
PAYLOAD
SPECIAL

75%⬇

BIT

SPECIAL PRICE

ON SALE!

RaaS Kit

+ customer
service

50%
less a
month!

Extortion Economics
Ransomware's new business model

Cyber Signals
August 2022

80%

○ Ransomware
attacks exploiting
configuration errors

Over 80 percent of
ransomware attacks can
be traced to common
configuration errors in
software and devices.[1]

INFOSTEALER MALWARE

SAVE

9 780201 379624

SALE

Password Bundle

200 pack

Buy one get one fre

Introduction

Cybercriminals emboldened by underground ransomware economy

While ransomware continues to be a headline-grabbing topic, there's ultimately a relatively small, connected ecosystem of players driving this sector of the cybercrime economy. The specialization and consolidation of the cybercrime economy has fueled ransomware as a service (RaaS) to become a dominant business model, enabling a wider range of criminals, regardless of their technical expertise, to deploy ransomware.

We are all cybersecurity defenders.

Security Snapshot

Microsoft's Digital Crimes Unit (DCU)
Directed the removal of more than 531,000 unique phishing URLs and 5,400 phish kits between July 2021 and June 2022, leading to the identification and closure of over 1,400 malicious email accounts used to collect stolen customer credentials.[1]

Email Threats:
Median time for an attacker to access your private data if you fall victim to a phishing email is one hour, 12 minutes.[1]

Endpoint Threats:
Median time for an attacker to begin moving laterally within your corporate network if a device is compromised is one hour, 42 minutes.[1]

New business model offers fresh insights for defenders

Threat briefing

Just as many industries have shifted toward gig workers for efficiency, cybercriminals are renting or selling their ransomware tools for a portion of the profits, rather than performing the attacks themselves.

The [Ransomware as a Service](#) economy allows cybercriminals to purchase access to Ransomware payloads and data leakage as well as payment infrastructure. Ransomware "gangs" are in reality RaaS programs like Conti or REvil, used by many different actors who switch between RaaS programs and payloads.

RaaS lowers the barrier to entry and obfuscates the identity of the attackers behind the ransoming. Some programs have 50+"affiliates," as they refer to users of their
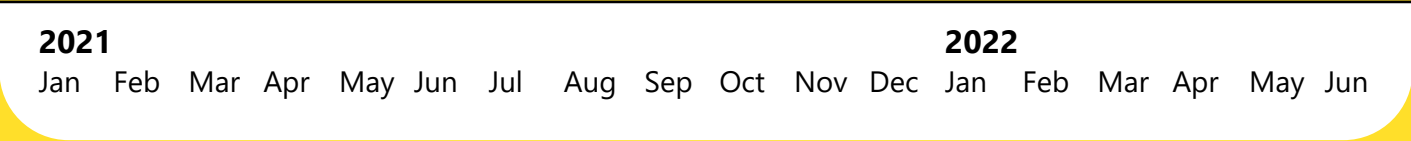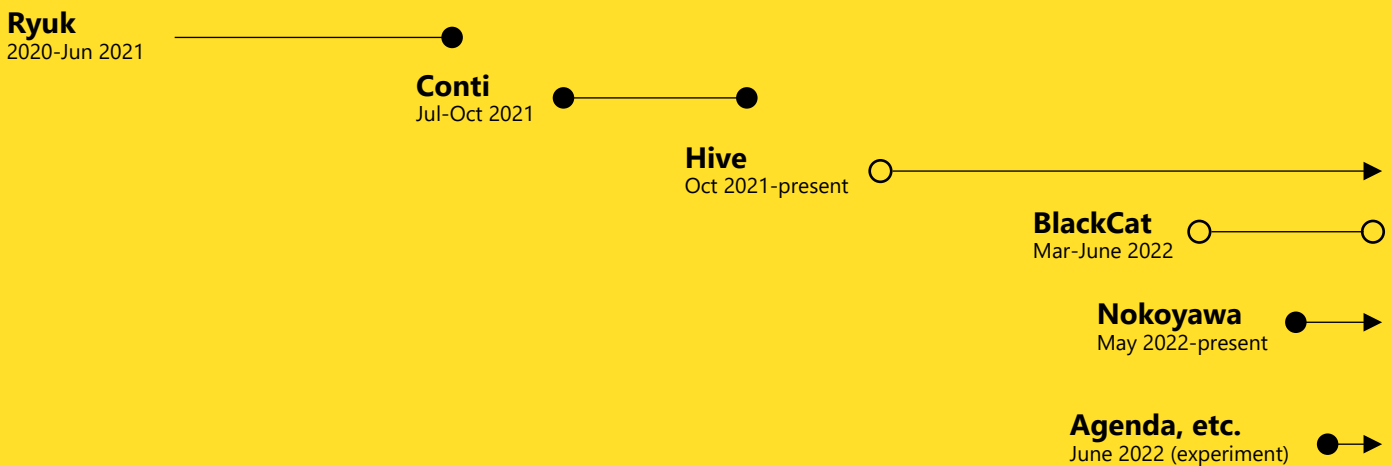
service, with varying tools, tradecraft, and objectives. Just as anyone with a car can drive for a rideshare service, anyone with a laptop and credit card willing to search the dark web for penetration testing tools or out-of-the-box malware can join this economy.

This industrialization of cybercrime has created specialized roles, like access brokers who sell access to networks. A single compromise often involves multiple cybercriminals in different stages of the intrusion.

RaaS kits are easy to find on the dark web and are advertised in the same way goods are advertised across the internet.

A RaaS kit may include customer service support, bundled offers, user

DEV-0237 ransomware payloads over time

Ryuk
2020-Jun 2021

Conti
Jul-Oct 2021

Hive
Oct 2021-present

BlackCat
Mar-June 2022

Nokoyawa
May 2022-present

Agenda, etc.
June 2022 (experiment)

2021
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec

2022
Jan Feb Mar Apr May Jun

reviews, forums, and other features. Cybercriminals can pay a set price for a RaaS kit while other groups selling RaaS under the affiliate model take a percentage of the profits.

Ransomware attacks involve decisions based on configurations of networks and differ for each victim even if the ransomware payload is the same. Ransomware culminates an attack that can include data exfiltration and other impact. Because of the interconnected nature of the cybercriminal economy, seemingly unrelated intrusions can build upon each other. Infostealer malware that steals passwords and cookies get treated with less severity, but cybercriminals sell these passwords to enable other attacks.

These attacks follow a template of initial access via malware infection or exploitation of a vulnerability then credential theft to elevate privileges and move laterally. Industrialization

allows prolific and impactful ransomware attacks to be performed by attackers without sophistication or advanced skills. Since the shutdown of Conti we've observed shifts in the ransomware landscape. Some affiliates who were deploying Conti moved to payloads from established RaaS ecosystems like LockBit and Hive, while others simultaneously deploy payloads from multiple RaaS ecosystems.

New RaaS like QuantumLocker and Black Basta are filling the vacuum left by Conti's shutdown. Since most Ransomware coverage focuses on payloads instead of actors, this payload switching is likely to confuse governments, law enforcement, media, security researchers, and defenders about who is behind the attacks.

Reporting on ransomware may seem like an endless scaling problem; however, the reality is a finite set of actors using the set of techniques.

Recommendations:

Build credential hygiene: Develop a logical network segmentation based on privileges that can be implemented alongside network segmentation to limit lateral movement.

Audit credential exposure: Auditing credential exposure is critical in preventing ransomware attacks and cybercrime in general. IT security teams and SOCs can work together to reduce administrative privileges and understand the level at which their credentials are exposed.

Reduce the attack surface: Establish attack surface reduction rules to prevent common attack techniques used in ransomware attacks. In observed attacks from several ransomware associated activity groups, organizations with clearly defined rules have been able to mitigate attacks in their initial stages while preventing hands on keyboard activity.

Cybercriminals add double extortion to attack strategy

Defending against attacks

Ransomware exists to extort payment from a victim. Most current RaaS programs also leak stolen data, known as double extortion. As outages cause backlash and government disruption of ransomware operators increases, some groups forgo ransomware and pursue data extortion.

Two extortion focused groups are DEV-0537 (aka LAPSUS$) and DEV-0390 (a former Conti affiliate). DEV-0390's intrusions initiate from malware but use legitimate tools to exfiltrate data and extort payment. They deploy penetration testing tools like Cobalt

Strike, Brute Ratel C4, and the legitimate Atera remote management utility to maintain access to a victim. DEV-0390 will escalate privileges by stealing credentials, locate sensitive data (often on corporate backup and file servers), and send the data to a cloud file sharing site using a file backup utility.

DEV-0537 uses a very different strategy and tradecraft. Initial access is obtained by purchasing credentials on the criminal underground or from employees at targeted organizations.

Problem

1 Stolen passwords and unprotected identities

More than malware, attackers need credentials to succeed. In nearly all successful ransomware deployments, attackers gain access to privileged, administrator level accounts granting broad access to an organizations' network.

2 Missing or disabled security products

In almost every observed ransomware incident, at least one system exploited in the attack had missing or misconfigured security products that allowed intruders to tamper with or disable certain protections.

3 Misconfigured or abused applications

You might use a popular app for one purpose, but that doesn't mean criminals can't weaponize it for another goal. Too often, "legacy" configurations mean an app is in its default state, allowing any user wide access across entire organizations. Don't overlook this risk or hesitate to change app settings for fear of disruption.

4 Slow patching

It's a cliché, like "Eat your vegetables!" – but it's a critical fact: The best way to harden software is to keep it updated. While some cloud based apps update with no user action, companies must apply other vendor patches immediately. In 2022 Microsoft observes that older vulnerabilities are still a primary driver in attacks.

Action

1 Authenticate Identities

Enforce multifactor authentication (MFA) on all accounts, prioritize administrator and other sensitive roles. With a hybrid workforce, require MFA on all devices, in all locations, at all times. Enable passwordless authentication like FIDO keys or Microsoft Authenticator for apps that support it.

2 Address Security Blind Spots

Like smoke alarms, security products must be installed in the correct spaces and tested frequently. Verify that security tools are operating in their most secure configuration, and that no part of a network is unprotected.

3 Harden internet facing assets

Consider deleting duplicative or unused apps to eliminate risky, unused services. Be mindful of where you permit remote helpdesk apps like TeamViewer. These are notoriously targeted by threat actors to gain express access to laptops.

4 Keep systems up to date

Make software inventory a continuous process. Keep track of what you are running and prioritize support for these products. Use your ability to patch quickly and conclusively to gage where transitioning to cloud based services is beneficial.

Understanding the interconnected nature of identities and trust relationships in modern technology ecosystems, they target telecommunications, technology, IT services, and support companies to leverage access from one organization to gain entry into partner or supplier networks. Extortion only attacks demonstrate that network defenders must look beyond end stage ransomware and keep a close eye on data exfiltration and lateral movement.

If a threat actor is planning to extort an organization to keep their data private, a ransomware payload is the least significant and least valuable part of the attack strategy. Ultimately, it's an operator's choice what they choose to deploy, and ransomware is not always the big ticket payout every threat actor is after.

While ransomware or double extortion can seem an inevitable outcome from an attack by a sophisticated attacker, ransomware is an avoidable disaster. Reliance on security weaknesses by attackers means that investments in cyberhygiene go a long way.

Microsoft's unique visibility gives us a lens into threat actor activity. Rather than rely on forum posts or chat leaks, our team of security experts studies new ransomware tactics and develops threat intelligence that informs our security solutions.

Integrated threat protection across devices, identities, apps, email, data, and the cloud helps us identify attacks that would have been labeled as multiple actors, when they're in fact a single set of cybercriminals. Our Digital Crimes Unit composed of technical, legal, and business experts continues to work with law enforcement to disrupt cybercrime.

Recommendations:

Harden the cloud: As attackers move toward cloud resources, it's important to secure these resources and identities as well as on-premise accounts. Security teams should focus on hardening security identity infrastructure, enforcing multifactor authentication (MFA) on all accounts, and treating cloud admins/tenant admins with the same level of security and credential hygiene as domain admins.

Prevent initial access: Prevent code execution by managing macros and scripts, and enabling Attack Surface Reduction Rules.

Close security blind spots: Organizations should verify that their security tools are running in optimum configuration and perform regular network scans to ensure a security product protects all systems.

Microsoft has in-depth recommendations at https://aka.ms/ransomware-as-a-service.

Expert Profile

Emily Hacker:
Threat intelligence analyst

Emily Hacker did not expect to become a threat intelligence analyst at Microsoft after studying journalism in college. Her first job in cybersecurity was as a technical writer at an oil and gas firm. "I was editing intelligence reports, intelligence presentations, and helping with incident metrics. Over the course of that first year, I became absolutely enthralled with the work that intelligence analysts do."

Emily's work at Microsoft began in 2020 as an analyst for Microsoft Defender for Endpoint and Microsoft Defender for Office. One of the focus areas for these teams is to protect customers from threats associated with ransomware. Emily is directly involved in many of the investigations that built Microsoft's knowledge of the RaaS economy and the access broker/operator/affiliate relationship, actively hunting for evidence of pre-ransomware signals.

"Following trends and techniques used by RaaS operators and their affiliates in the pre-ransom phase of an incident is critical to protecting customers from these types of threats," she said. "My job is to spot these pre-ransomware actors as early as possible. If you are only looking for the ransomware payload, itself—you're too late."

To stay on top of the changing RaaS landscape, Emily and her team use a combination of automated systems and human analysis to analyze, escalate, and act on logs, alerts, and other activity in real time. Emily's team helps anticipate, pre-empt, and respond to different incidents on the front lines

of customers' networks, while also contributing to MSTIC's ever growing assessment of ransomware linked actor tools, motives, and strategies.

When it comes to a ransomware incident, the stakes can be incredibly high. Ransomware operators are known to target critically important networks related to education, transportation, healthcare, or telecommunications systems. When these networks are affected, the results can be catastrophic.

"The work we do at Microsoft to track and prevent ransomware incidents is important because we're protecting not just our customers, but their customers as well," Hacker said. "Identifying the tools and techniques associated with ransomware and pre-ransomware incidents as early as possible is critical when these incidents have potentially wide-reaching consequences for companies, their employees, and their customers."

> " My job is to spot these pre-ransomware acts as early as possible. If you are only looking for the ransomware payload, itself—you're too late."
>
> Threat intelligence analyst
> **Emily Hacker**

Microsoft

1. Methodology: For snapshot data, Microsoft platforms, including Defender and Azure Active Directory, and our Digital Crimes Unit provided anonymized data on threat activity, such as malicious email accounts, phishing emails, and attacker movement within networks. Additional insights are from the 43 trillion daily security signals gained across Microsoft, including the cloud, endpoints, the intelligent edge, and our Compromise Security Recovery Practice and Detection and Response teams. Cover art is representative of the affiliate business model. Percentages do not represent actual discounts. Cover stat is based on Microsoft engagements over the past year.