Microsoft Security

Ransomware-as-a-Service: The new face of industrialised cybercrime

Cybercrime's newest business model, human-operated attacks, emboldens criminals of varying ability.

Ransomware, one of the most persistent and pervasive cyber threats, continues to evolve, and its latest form presents a new menace to organisations worldwide. The evolution of ransomware doesn't involve new advances in technology. Instead, it involves a new business model: Ransomware-as-a-Service (RaaS).

Ransomware-as-a-Service (RaaS) is an arrangement between an operator, who develops and maintains the tools to power extortion operations, and an affiliate, who deploys the ransomware payload. When the affiliate conducts a successful ransomware and extortion attack, both parties profit.

The RaaS model lowers the barrier to entry for attackers who may not have the skill or technical wherewithal to develop their own tools, but can manage ready-made penetration testing and sysadmin tools to perform attacks. These lower-level criminals can also just buy network access from a more sophisticated criminal group that has already breached a perimeter.

Although RaaS affiliates use ransomware payloads provided by more sophisticated operators, they are not part of the same ransomware 'gang'. Rather, these have their own distinct enterprises operating in the overall cybercriminal economy.

Advancing the capabilities of cybercriminals and growing the overall cybercriminal economy

The Ransomware-as-a-Service model has facilitated a rapid refinement and industrialisation of what less capable criminals can accomplish. In the past, these less sophisticated criminals may have used commodity malware they either built or purchased to perform attacks that are limited in scope, but now they can get everything they need – from access to networks to ransomware payloads – from their RaaS operators (for a price, of course). Many RaaS programs further incorporate a suite of extortion support offerings, including leak site hosting and integration into ransom notes, as well as decryption negotiation, payment pressure and cryptocurrency transaction services.

This means that the impact of a successful ransomware and extortion attack remains the same regardless of the attacker's skills.

Discovering and exploiting network vulnerabilities… for a price

One way RaaS operators provide value to their affiliates is by providing access to compromised networks. Access brokers scan the internet for vulnerable systems, which they can compromise and reserve for later profit.

In order to be successful, attackers need credentials. Compromised credentials are so important to these attacks that when cybercriminals sell network access, in many instances, the price includes a guaranteed administrator account.

What the criminals do with their access once it has been achieved can vary wildly depending on the groups and their workloads or motivations. The time between initial access to a hands-on keyboard deployment can therefore range from minutes to days or longer, but when the circumstances permit, damage can be inflicted at breakneck speed. In fact, the time from initial access to full ransom (including handoff from an access broker to an RaaS affiliate) has been observed to take less than an hour.

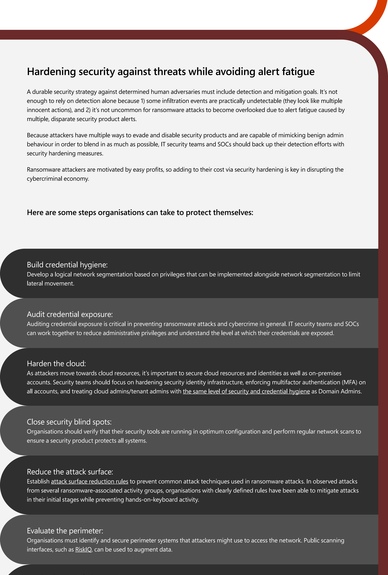
Keeping the economy moving – persistent and sneaky access methods

Once attackers gain access to a network, they are loathe to leave – even after collecting their ransom. In fact, paying the ransom may not reduce the risk to an affected network and potentially only serves to fund cybercriminals, who will continue trying to monetise attacks with different malware or ransomware payloads until they are evicted.

The handoff that transpires between different attackers as transitions in the cybercriminal economy occur means that multiple activity groups may persist in an environment using various methods disparate from the tools used in a ransomware attack. For example, initial access gained by a banking trojan leads to a Cobalt Strike deployment, but the RaaS affiliate that purchased the access may choose to use a remote access tool such as TeamViewer to operate its campaign.

Using legitimate tools and settings to persist versus malware implants such as Cobalt Strike is a popular technique among ransomware attackers to avoid detection and remain resident in a network for longer.

Another popular attacker technique is to create new backdoor user accounts, whether local or in Active Directory, that can then be added to remote access tools such as a virtual private network (VPN) or Remote Desktop. Ransomware attackers have also been observed editing the settings on systems to enable Remote Desktop, reduce the protocol's security and add new users to the Remote Desktop Users group.



Facing the most elusive and cunning adversaries in the world

One of the qualities of RaaS that makes the threat so concerning is how it relies on human attackers who can make informed and calculated decisions and vary attack patterns based on what they find in the networks where they land, ensuring they meet their goals.

Microsoft coined the term human-operated ransomware to define this category of attacks as a chain of activity that culminates in a ransomware payload, not as a set of malware payloads to be blocked.

While most initial access campaigns rely on automated reconnaissance, once the attack shifts to the hands-on-keyboard phase, attackers will use their knowledge and skill to try to defeat the security products in the environment.

Ransomware attackers are motivated by easy profits, so adding to their cost via security hardening is key in disrupting the cybercriminal economy. This human decision-making means that even if security products detect specific attack stages, the attackers themselves don't get fully evicted; they attempt to continue if not blocked by a security control. In many instances, if a tool or payload is detected and blocked by an antivirus product, attackers simply grab a different tool or modify their payload.

Attackers are also aware of security operations centre (SOC) response times and the capabilities and limitations of detection tools. By the time the attack reaches the stage of deleting backups or shadow copies, it would be minutes away from ransomware deployment. The adversary would likely have already performed harmful actions like the exfiltration of data. This knowledge is key for SOCs responding to ransomware: investigating detections like Cobalt Strike before the ransomware deployment stage and performing swift remediation actions and incident response (IR) procedures are critical for containing a human adversary.

Hardening security against threats while avoiding alert fatigue

A durable security strategy against determined human adversaries must include detection and mitigation goals. It's not enough to rely on detection alone because 1) some infiltration events are practically undetectable (they look like multiple innocent actions), and 2) it's not uncommon for ransomware attacks to become overlooked due to alert fatigue caused by multiple, disparate security product alerts.

Because attackers have multiple ways to evade and disable security products and are capable of mimicking benign admin behaviour in order to blend in as much as possible, IT security teams and SOCs should back up their detection efforts with security hardening measures.

Ransomware attackers are motivated by easy profits, so adding to their cost via security hardening is key in disrupting the cybercriminal economy.

Here are some steps organisations can take to protect themselves:

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.

Harden the cloud:
As attackers move towards cloud resources, it's important to secure cloud resources and identities as well as on-premises 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.

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

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, organisations with clearly defined rules have been able to mitigate attacks in their initial stages while preventing hands-on-keyboard activity.

Evaluate the perimeter:
Organisations must identify and secure perimeter systems that attackers might use to access the network. Public scanning interfaces, such as RDP, can be used to augment data.

Harden internet-facing assets:
Ransomware attackers and access brokers use unpatched vulnerabilities, whether already disclosed or zero-day, especially in the initial access stage. They also rapidly adopt new vulnerabilities. To further reduce exposure, organisations can use the threat and vulnerability management capabilities in endpoint detection and response products to discover, prioritise and remediate vulnerabilities and misconfigurations.

Prepare for recovery:
The best ransomware defence should include plans to recover quickly in the event of an attack. It will cost less to recover from an attack than to pay a ransom, so be sure to conduct regular backups of your critical systems and protect those backups against deliberate erasure and encryption. If possible, store backups in online immutable storage or fully offline or off-site.

Further defence against ransomware attacks

The multi-faceted threat of the new ransomware economy and elusive nature of human-operated ransomware attacks require organisations to adopt a comprehensive approach to security.

The steps we outlined above help defend against common attack patterns and will go a long way in preventing ransomware attacks. To further stiffen defences against traditional and human-operated ransomware and other threats, use security tools that can provide deep cross-domain visibility and unified investigation capabilities.

For an additional overview of ransomware complete with tips and best practices for prevention, detection and remediation, see Protect your organisation from ransomware, and for even more in-depth information on human-operated ransomware, read Senior Security Researcher Jessica Payne's Ransomware-as-a-Service: Understanding the cybercrime gig economy and how to protect yourself.

Stay on top of evolving security issues by visiting Security Insider.

Share this infographic:

Microsoft