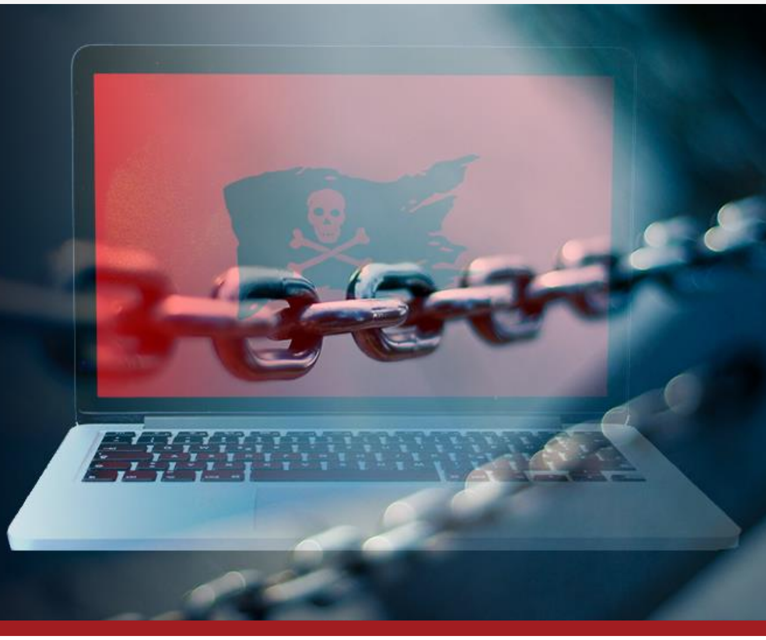
ACALVIO

SOLUTION BRIEF

Acalvio ShadowPlex Ransomware Protection

How security teams can defend against evolving ransomware variants and protect their sensitive data



Evolution in ransomware: Ransomware as a Service (RaaS) generates custom variants

Ransomware threats have evolved, with Ransomware as a Service (RaaS) threat groups creating unique ransomware variants to execute stealthy attacks.

This represents a significant shift from the early ransomware variants that had a fixed malware payload that was deployed for each campaign. Modern ransomware is human operated, with the threat actor bringing human skill and sophisticated tooling to generate custom ransomware variants..

Overview of RaaS model

RaaS model involves a decentralized model for ransomware. Ransomware has been turned into an industry, with specialization for each threat actor group involved in this operation.

The RaaS model includes:

Initial Access Brokers (IABs): IABs are the group that is responsible for obtaining and providing the initial access to the ransomware threat actors. IABs provide direct access to an organization, enabling the threat actor to gain an initial foothold that is a guaranteed point of entry to the organization.

RaaS Operators: the group that is responsible for building the tooling for ransomware, this is provided to the RaaS affiliates. RaaS operators specialize at building sophisticated ransomware tooling and provide an ability for RaaS affiliates to customize this tooling for specific campaigns.

RaaS affiliates: human threat actors that are responsible for executing the specific ransomware campaign. RaaS affiliates customize the ransomware payload, perform pre-ransom stage exploits, detonate the ransomware payload and negotiate ransom payments.

Initial Access Brokers (IABs) provide trusted access

The evolution of ransomware to adopt a decentralized, RaaS model introduces significant implications for defense teams. IABs have evolved to allow RaaS affiliates to pay for and obtain highly specific levels of access, for example, a RaaS affiliate can specify that they would want to gain access to a jump server as the initial access point and the jump server should be one that does not have endpoint detection and response (EDR) or Antivirus (AV) on it. By gaining this access, the RaaS affiliate has the ability to leverage the jump server as the pivot point for the entire ransomware campaign. The lack of security defenses on such a jump server enables the RaaS affiliate to download known malware (that would otherwise have been blocked) and use this malware for lateral movement, vulnerability exploits.

RaaS operators are leveraging modern programming languages to evade detection

RaaS operators have adapted to the use of modern programming languages, such as Rust and Golang to build ransomware tooling. As an example, the *Sphynx* variant of the Alphv ransomware was rewritten in Rust. The use of modern programming languages is gaining in popularity among RaaS operators due to the lack of signatures written for these languages.

.

Early ransomware versions were primarily implemented in C and C++ as programming languages. As a result, the signatures for detecting ransomware (available in AV) are primarily written for malware implemented in C and C++.

Modern ransomware are moving to the new programming languages and evading signature-based detection. RaaS operators are also adopting the use of signed kernel drivers for the ransomware payloads to evade detection by EDR. RaaS operators are specialists in building ransomware tooling and generate new versions with significant changes and enhancements, making it harder for detection engineering teams to keep pace through traditional detection approaches.

As an example, the Lockbit ransomware group has built Lockbit 1.0, 2.0, 3.0, Lockbit Green, Lockbit for Mac as major version updates with significant different capabilities and implementation.

RaaS affiliates leverage stealthy techniques to bypass traditional security solutions

RaaS affiliates perform minor customizations to the tooling built by the RaaS operators to generate custom payloads. These minor customizations are sufficient to evade detection techniques that are focused on identifying malware based on evidence of known payloads.

RaaS affiliates are leveraging stealthy offensive techniques to evade detection by traditional security solutions. These include: use of valid credentials for lateral movement, exploits targeting unmanaged endpoints, disabling agent-based security controls, clearing log evidence.

Disabling agent-based security controls is a popular technique adopted by modern ransomware. RaaS affiliates perform minor customizations to provide a list of specific services that need to be disabled for a given organization. After gaining initial access, RaaS affiliates escalate privileges and disable AV, EDR, other forms of agent-based security monitoring.

Identity-driven attacks are another effective approach leveraged by RaaS affiliates for lateral movement and propagation. Traditional security solutions are unable to distinguish between legitimate and malicious use of credentials, making this an effective approach for ransomware propagation.

Why traditional security solutions are unable to keep pace

Modern ransomware bypass prevention-based security controls such as the perimeter firewalls through the guaranteed initial access provided by the IABs. Threat actors gain access to a jump server in the DMZ that serves as the initial entry point for ransomware.

For threat detection, traditional security solutions are focused detecting known threats with known attack TTPs. These solutions were effective against the early versions of ransomware that had fixed set of payloads being used. With the evolution of ransomware to adopt a RaaS model and generating custom payloads, traditional security solutions are falling short and are unable to detect evolving variants or are very slow at raising alerts, leaving the organization vulnerable as ransomware propagates.

The use of double and triple extortion techniques have significant implications for cyber defense

Ransomware threats have moved away from the initial focus on data encryption followed by ransom payment demands in exchange for decryption keys.

Ransomware groups are employing double extortion and triple extortion techniques that involve data exfiltration and distributed denial of service (DDoS) attacks, in addition to the encryption. This aggressive strategy employed by the threat actors has significant implications for cyber defense.

Ransomware groups are leveraging the reputation damage and leakage of sensitive corporate data to drive up ransom payments significantly.

Acalvio ShadowPlex: Active Defense platform based on cyber deception and AI

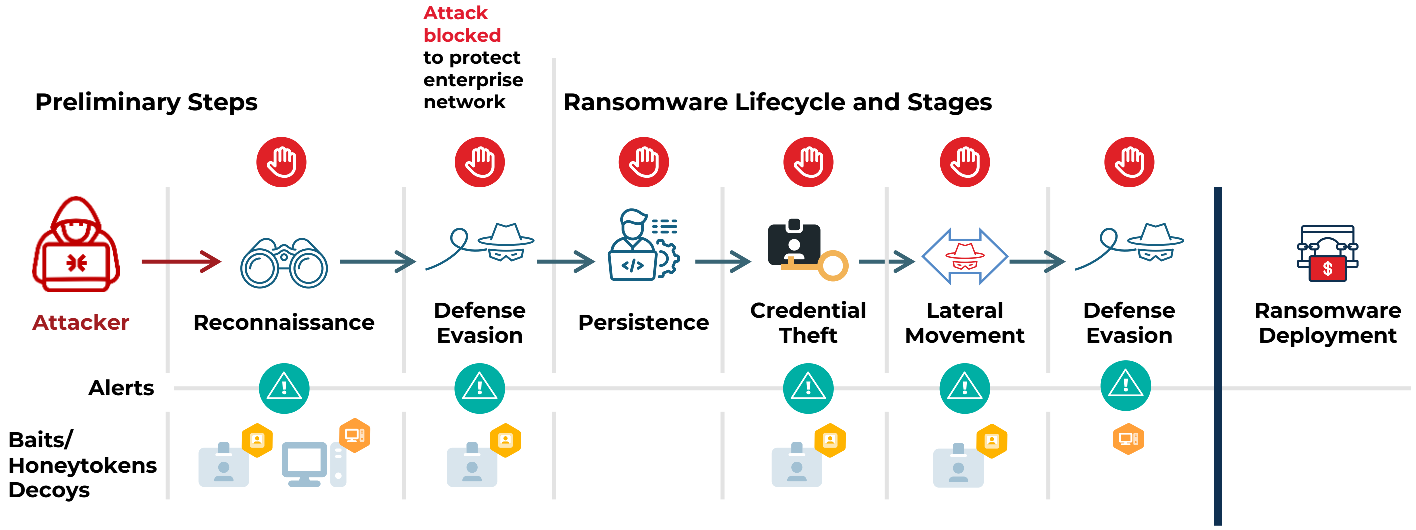
Acalvio ShadowPlex is a robust and proven Active Defense platform that combines cyber deception and AI to enable organizations to defend against a wide variety of threats.

Cyber deception is based on setting relevant traps for the threat actor and observing for interactions with these traps. Deceptions are not used for existing IT or business workflows; any usage of the deceptions is an immediate indicator of malicious activity. Deceptions are agnostic to attacker TTPs and can detect evolving threats with precision. Acalvio ShadowPlex has a rich palette of prebuilt deceptions, including decoys (network deceptions), breadcrumbs (deceptive profiles on endpoints that lead attackers to decoys), baits (tripwires that alert on access), honey accounts (deceptive user accounts and service accounts added to identity stores) and honeytokens (deceptive credential profiles on endpoints).

Ransomware threat detection with Acalvio ShadowPlex

Acalvio ShadowPlex provides a prebuilt playbook for Ransomware Protection. This playbook contains a set of purpose-built deceptions to detect ransomware threats with precision. The deception playbook deploys deceptions for each stage of the ransomware lifecycle, the deceptions are placed strategically and are attractive for the threat actors to exploit. By deploying deceptions on endpoints, in identity stores, and at the network, defense teams can gain visibility to ransomware threats at the pre-ransom stage, enabling response actions to block the threat and prevent attack propagation.

Deception Detects Ransomware with Precision



The proven approach to ransomware threat detection provides important benefits to organizations. This includes:

Detect known and unknown (zero-day) ransomware variants

ShadowPlex ransomware threat detection is based on deception technology. Deception-based threat detection is agnostic to attacker TTPs and brings an important benefit of detecting unknown, zero-day variants in addition to known ransomware variants. ShadowPlex detection of ransomware is independent of the signatures, programming language, cryptographic algorithms, or specific attack TTPs leveraged by the ransomware. ShadowPlex complements traditional security solutions for a defense in depth approach to ransomware protection. ShadowPlex, with the rich set of purpose-built deceptions, provides visibility for the evolving variants generated by RaaS operators and affiliates that bypass traditional security solutions. The approach is future proof, as new ransomware variants emerge, ShadowPlex will continue to detect these variants. Defense teams can leverage traditional layers for attribution of the ransomware, ShadowPlex has prebuilt integrations with these solutions to augment the detection with the attribution.

Early treat detection at pre-ransom stage

ShadowPlex deceptions include baits and honeytokens deployed on endpoints and in identity stores. Human-operated ransomware gains initial access to an organization and performs an initial offensive sequence to gain access to credentials for lateral movement and to identify targets for propagation. The offensive lifecycle includes reconnaissance, credential access, privilege escalation, defense evasion, persistence as some of the techniques that are used prior to propagation and lateral movement. Through the deployment of a set of purpose-built deceptions at scale, defense teams gain the benefit of early detection of ransomware, at pre-attack stage. With prevention-solutions being bypassed by IABs, an effective defense strategy.

Precise and actionable alerts

ShadowPlex detections for ransomware are high-fidelity and precise. The detections are immediately actionable by SOC teams, eliminating the need for manual alert deduplication or correlation that is associated with traditional detection approaches. SOC teams can avoid the alert deluge and gain actionable alerts. With ransomware threats leveraging rapid execution speeds, it is essential for SOC to act rapidly, and the precise alerts raised by ShadowPlex enables SOC to take immediate response actions.

Automated Response actions

ShadowPlex provides automated response actions to isolate the threat and protect the organization. The response actions are performed through prebuilt integrations of ShadowPlex with security and network management platforms in the organization. Automated response actions are contingent to a high level of confidence on the fidelity of the threat detection and the absence of associated false positives. ShadowPlex, through its purpose-built deceptions, detects ransomware with speed and precision, providing the foundation to enable automated response policies to be configured by SOC teams. ShadowPlex automated response isolates the endpoint and prevents ransomware propagation. By combining the benefits of the early threat detection (including at pre-ransom stage) and automated response actions, organizations gain the benefit of an active and comprehensive approach for ransomware defense.

ShadowPlex: enterprise-scale deception for comprehensive ransomware defense

Ransomware can target any part of the organization as the point of initial access. Defense teams would be interested in detecting the threat at pre-ransom stage to prevent attack propagation. It is essential to deploy deception at scale, across the organization to be able to detect the threat at or near the point of initial access. To deploy deception at scale, organizations need a platform. ShadowPlex provide enterprise-scale deception technology that protects the organization from ransomware. ShadowPlex provides purpose-built deceptions along with a pre-packaged ransomware protection playbook to provide immediate time to value. The playbook deploys deceptions to detect ransomware at each stage of the attack lifecycle, providing early detection of the threat. ShadowPlex uses AI algorithms to recommend deceptions that are realistic for the target environment. ShadowPlex is an agentless platform, eliminating the management and security challenges associated with the deployment of additional agents. ShadowPlex performs automated triaging of deception events to generate high-fidelity, actionable alerts for SOC teams. The alerts are mapped to the MITRE ATT&CK framework for standardized incident response. Automated response policies can be configured to block the threat and prevent ransomware propagation.

ShadowPlex, through its powerful deception-based ransomware defense, protects organizations from known and unknown(zero-day) ransomware variants. The approach is future proof, enabling the organizations to stay protected as new variants of ransomware emerge.

Acalvio, the leader in cyber deception technology, helps enterprises actively defend against advanced security threats. Acalvio Active Defense Platform, built on 25 issued patents in autonomous deception and advanced AI, provides robust solutions for Identity Threat Detection and Response (ITDR), Advanced Threat Detection, OT Security, Zero Trust, Active Directory Protection and Ransomware Protection. The Silicon Valley-based company's solutions serve Fortune 500 enterprises, government agencies and are available to deploy
on-premises, in the cloud or via marquee managed service providers. For more information, please visit **www.acalvio.com**