illusive

Solution Brief

Ransomware

A Global Data Pandemic

Recent high-profile ransomware attacks offer clear evidence that the attackers have the upper hand in the battle for access to corporate networks, systems, and critical services.

Three facets reveal a significant imbalance between attackers and defenders, creating a Global Data Pandemic:

1 **Automation** Ransomware-as-a-Service (RaaS) reduces the barriers for bad actors perpetrating ransomware attacks. They no longer require programming skills to launch an attack.

2 **Anonymized Cash Flow** A thriving, and largely unregulated cryptocurrency market allow attackers to receive untraceable payments.

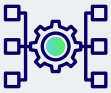
3 **Routine Behaviors** Deficient security hygiene and lateral movement detection capabilities allow attackers to operate inside a customer's environment largely unchecked.

The first two are well beyond IT security teams' control; however, deploying an Active Defense to improve security hygiene and lateral movement detection can change the game on ransomware attackers. If your environment is like most:

1 in 5 endpoints contain cached privileged account credentials (e.g., Domain Admins)

37% of endpoints contain policy violating credential and connection information.

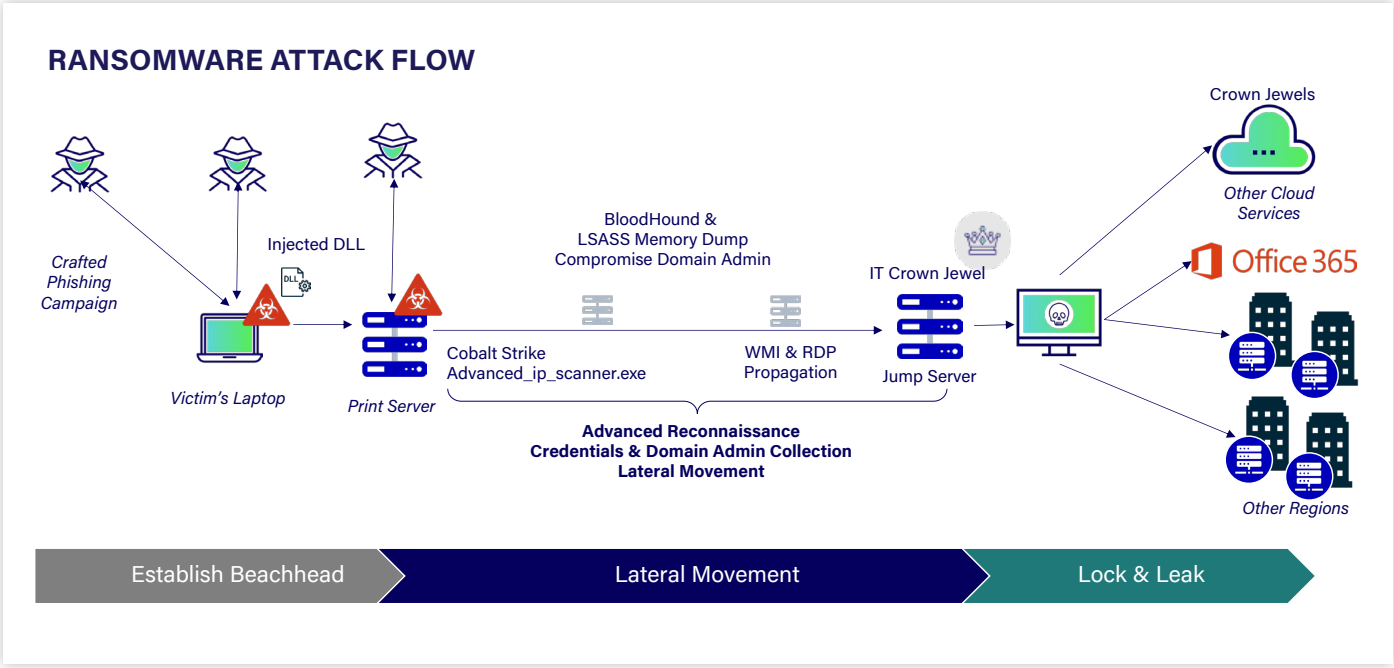
Everything the attacker sees is real and potentially helpful in deploying ransomware



'Living Off The Land' attack techniques go largely undetected by security controls like endpoint detection and response (EDR)

The business requirements for efficient IT support necessitates active administrator privileged sessions and connections to continue as a mainstay for IT teams. A byproduct of administrative remote access is actively cached credential and connection information that is easily exploited by attackers. Today's ransomware attackers harvest this information to aid their reconnaissance, identify ransom targets, and escalate the privileges necessary to lock and leak data.

Attackers that 'live off the land', operate with legitimate credentials and do what a user does when they do it to perform reconnaissance, move laterally, and escalate privileges are not doing anything unusual and thus are not easily detected. Moreover, sophisticated attackers are utilizing techniques to scan for the presence of and disabling installed endpoint security controls such as EDR.



It is better to detect the attacker before they successfully move laterally and reach any targeted crown jewel system(s). Once a beachhead has been established, the attacker will engage in post-exploitation TTPs to harvest credentials, move laterally, and escalate privileges to gain access to crown jewel targets that enable them to distribute ransomware to the whole organization.

The process of dumping LSASS memory, using the attacker tool suite Cobalt Strike, and WMI/RDP propagation are common TTPs used in both recent ransomware and the SolarWinds attacks. These techniques, represented by steps 6 through 9 of the MITRE ATT&CK framework, are common to nation-state, ransomware, and insider threats alike.

Implementing an Active Defense will significantly reduce ransomware risk by preventing the attacker from performing the reconnaissance and lateral movement required to escalate privileges and do major damage.

Imagine how much more difficult it would be on attackers if the useful cached information is gone and **90% of what they see is deceptive.**

IDENTITY RISK MANAGEMENT

Enables organizations to create an environment hostile to ransomware attacker activities by:

1 Stopping attackers from moving laterally before they can reach a crown jewel and encrypt.

2 Automatically mitigating the initial encryption event on real asset with a ransomware deception.

Identity Risk Management is a vital part of a diversified detection strategy, filling important hygiene and attacker lateral movement detection gaps in existing defenses. Unlike agent-based security controls, Illusive's agentless architecture prevents attackers from detecting its presence so they are unable to disable or takeover Illusive Identity Risk Management, while also incorrectly assuming that they are stealthily operating in an environment. Each of the products in the Identity Risk Management Suite play an important role in preventing ransomware attackers from achieving their objectives, accelerating the time to detection for an attacker before damage is done.

DISCOVER

Makes it difficult to 'live off the land' by continuously identifying and removing unnecessary credentials and pathways that are the fuel for the ransomware attacker to move laterally, escalate privileges and encrypt.

REMEDIATE

Makes it impossible for ransomware attackers to move laterally by transforming every endpoint into a web of deceptions. ADS deterministically accelerates threat detection by identifying threats based on attacker interaction with deceptions, not probabilistic controls based on signatures or behaviors. Ransomware-specific deceptions, a part of Illusive's Ransomware Guard, can be deployed throughout the network to protect your data from encryption.

PROTECT - When an attacker is on a real asset and initiates encryption activities, the process is redirected to encrypting deceptive documents, limiting impact to a small subset of systems. An alert is immediately generated, triggering an automated response, launching real-time source-based forensics from the Attack Intelligence System to gather data on the attacker.

IDENTITY RISK MANAGEMENT

Accelerates investigation and remediation with human readable on-demand telemetry for current ransomware attacker activities as it is occurring.

- In-progress screenshots of attacker activity
- Tool sets in use
- Command-and-control information
- Deployed files
- Process summary
- Registry information
- Active Directory details
- Chronological timeline of the attack

Attack Technique	Illusive Identity Risk Management
Disabling Endpoint Security (EPP/EDR)	No Agent to Disable or Avoid
Bypassing Anomaly Detection (Living off the Land)	Forced Detection through Deception
Domain Admin Collection	Discovery & Elimination of Cached Domain Admins
Shadow & Local Admin Collection	Discovery & Elimination of Shadow & Unmanaged Local Admins
Azure Admin Collection	Discovery & Elimination of Over-Privileged Azure Admins
LSASS Memory Dump	Windows Credential Deceptions
IP Scanner	Port Scanning and SMB Deceptions
Crown Jewel Credential Harvesting	RDP, SSH, FTP, Browser Deceptions
DCSync Activity	Discovery & Elimination of Unnecessary High-Privileged Accounts