SecurityFirst™
Protecting Critical Data

WHITE PAPER

Ransomware Protection

Effective Cybersecurity Hygiene

After years of experimentation, cybercriminals have leveraged the anonymity of Tor and the un-traceability of Bitcoin payments to converge on a favorite new attack tactic. Six of ten new attacks involve ransomware which can be quickly and brainlessly deployed with a high probability of achieving success. There's even a bustling marketplace on the Dark Web for purchasing this malware, with prices ranging from $0.50 to $3,000 helping developers earn upwards of $100,000 per year. And the best part of these crimes is that there's no middleman required, no need to exfiltrate data and sell it to other cybercriminals to enjoy the spoils.

What is Ransomware?

Ransomware is a form of malware that invades a victim's server or endpoint and holds the system or data hostage unless a ransom is paid—usually a reasonable amount, based on a perceived ability to pay to encourage cooperation. Simple versions of this malware may just lock the system or hijack a browser in a way any knowledgeable person can easily reverse. Stronger variants can employ a technique called cryptoviral extortion, encrypting a victim's files and potentially exfiltrating private data adding public disclosure to the list of possible perils befalling anyone who refuses to pay up.

Ransomware attacks can be carried out using a Trojan that is disguised as a legitimate file a user is fooled into downloading when it arrives as an email attachment. Other attack vectors include website links and one of the most widespread infections, last year's "WannaCry" worm, automatically traveled between computers without user interaction using open TCP ports. And it's not hard to get into the game. A recent study[1] found 6,300+ dark web marketplaces selling as many as 45,000 product listings.

The enduring popularity of this attack can be attributed to a general willingness to pay. Downtime in certain industries can be life threatening, and the ransom amounts are believed to be cheaper than costs required to establish an adequate defense as many organizations have outdated perspectives on data-centric security technology. But the wrinkle here is that paying once is somewhat like the dues associated with a professional or social organization. Yes indeed, you've joined an exclusive club.

Why Don't My Existing Cybersecurity Defenses Stop It?

The early days of building out an organization's cybersecurity program were consumed by deploying technologies that can basically be described as perimeter defenses. The general tactic was to keep the bad guys out using identity management, antivirus, firewalls and intrusion prevention systems. All were helpful and are still required today because the cybercriminal will take the path of least resistance to disrupt your business and steal any valuable information.

As known and publicly reported vulnerabilities continued to mount, security teams began to accept the idea that network perimeters were just no longer defendable, and the addition of mobile (BYOD) endpoints and social websites were making matters far worse. Consequently, a next level of investment focused on anomaly detection or the ability to determine when suspicious, never previously observed behaviors were occurring. Another important capability, but mostly effective against attackers who'd pierced the perimeter and were still searching the network for any information worth stealing.

Ransomware is effective because it typically bypasses these perimeter defenses and quickly begins to compromise your assets and disrupt operations before any anomalies surface. The nature (external value) of the data is more-or-less a secondary concern and for most shops, there are no remaining defenses in-place to protect it. Effective security systems are comprised of layers of protection, including data-centric technologies forming that last line of defense. Attacks like ransomware, regulations like GDPR, and decrees like Executive Order 13800 are all driving a new shift in spending focused on protecting your most valuable asset—digital data.

How Do I Defend Against It?

Conventional wisdom says do not pay the ransom; there's no guarantee you'll recover your systems and data. Many organizations that pay do recover their data, but it's not a case of honor among thieves. The cybercriminals are just hoping to come back in the future, betting you'll soon again be vulnerable.

According to the Department of Homeland Security (DHS)—among others—the only effective means for mitigating damages associated with a ransomware attack is to employ a data backup and recovery plan for all critical information.[2] Other recommendations include user education, frequent OS and application patching, penetration testing, applying the principle of "Least Privilege" to all systems and services, and regularly updating antivirus definitions—the standard litany. But none of these preventions help when your data is both exfiltrated and encrypted by the attackers.

A better solution incorporates data protection by what new regulations deem 'design and default.' It's sort of the same logic that led security teams to add anomaly detection when they realized perimeters were almost defenseless. Firstly, assume you will eventually be breached and protect your data proactively so no public data disclosure or sale to a third party is possible. A strong data-centric solution that couples encryption with access controls, logging and auditing will render the data useless to the hacker.

Secondly, once your data becomes maliciously encrypted, it's generally not recoverable without acquiring the exact decryption key. Further, if someone gets a Trojan or malicious macro into your network, basically past your firewall, then anything in that environment would most likely be affected including your on-line backups. The solution is to take down and rebuild the asset(s) using data stored OUTSIDE your network.

Apply Protection by Design and Default

The growing sophistication and proliferation of ransomware has many organizations assuming an attack is inevitable, but the reality is that many of these same organizations are still unprepared. Protecting against ransomware requires implementing good security hygiene to manage the health and quality of your data throughout its lifecycle. This means applying timely updates and patches, properly configuring firewalls, managing how networks, servers and data are accessed, using up-to-date anti-malware software and making sure your critical data assets are encrypted in transit and at rest, as well as backed up on a regular basis.

SecurityFirst's DataKeep™ is an integrated data-centric solution suite that provides all the tools one needs to significantly reduce risk associated with sensitive digital data while keeping costs under control. It's a drop-in technology that will complement any existing, format-preserving protection solutions designed for structured data, store decryption keys within a KMIP-compatible hardware store, log data access permits and denies to a SIEM solution, and permit automated operations via a RESTful API.

DataKeep uses customer-defined policies that manage who, what, when, where and how users access decrypted data. DataKeep allows you to define access policies that can be as narrow as -- a specific user, can only see specific data decrypted, when using a specific hashed process/application on a specific server. Policies use role-based access (RBAC), privileged access management (PAM) and default to least privileged access (LPA) so only those needing data access are allowed. Access can also be limited through specific applications. DataKeep encrypts data-at-rest on servers at a volume or file-level, on network file systems and prior to sending data to S3 object storage. DataKeep combines AES-256 encryption and internal key management that is certified to be FIPS 140-2 compliant.DataKeep logs all user data access requests, whether approved or denied, in real time to allow for prompt remediation. Event logs can be forwarded to Systems Information and Event Management (SIEM) for analysis and reporting.

In summary, SecurityFirst delivers data-centric solutions that address the high-profile cyber threats facing organizations today including data breaches and ransomware attacks. We emphasize protection of the data itself to serve as your last line of defense. Data is always protected no matter where it resides and recoverable in the event of an unexpected failure or malicious attack. As organizations and governments mandate stricter requirements for data privacy, SecurityFirst helps protect data from compromise and exposure. Don't settle for less; ransomware attack mitigation and recovery are within our data protection wheelhouse.

About SecurityFirst

SecurityFirst™ delivers data-centric solutions that address the high-profile cyber threats facing organizations today, such as data breaches, ransomware and cloud security. We emphasize protection of the data itself to serve as your last line of defense. Data is always protected no matter where it resides and recoverable in the event of an unexpected failure or malicious attack such as malware or ransomware. As organizations and governments mandate stricter requirements for data privacy, SecurityFirst helps protect data from compromise and exposure.

About DataKeep

DataKeep™secures critical data at its core to deliver unrivaled protection, control and resiliency. Customer-defined access policies, strong encryption and event logging combine with native secure backup/restore capabilities to address your data privacy, compliance and recovery needs.

Security teams can define and log access policies by job role and manage privileged and superuser access to block insider and external threats. DataKeep securely protects data at the source no matter where data resides, encrypting data at the volume or file level for attached storage or before sending to object storage. Native backup and restore commands can be leveraged to enable prompt recovery of archived data in the event of a ransomware attack.

DataKeep's ability to support M of N distributed shares allows companies to encrypt, split and distribute data across multiple object store locations or vendors for business continuity and operational efficiency. Organizations can utilize the backup and restore capabilities with object storage for secure cloud backup and archiving to improve resiliency. Secure your most valuable assets – your data, your brand and your reputation – with Datakeep.

Sources

1. Carbon Black's The Ransomware Economy
2. US Cert Alert (TA16-091A), Ransomware and Recent Variants

SecurityFirst™
Protecting Critical Data

For a product demonstration or more information call 1-888-884-7152

securityfirstcorp.com

80-20678-000 Rev. A0