Industry Security Brief

MERLINCRYPTION®

Protect Your Privates

Overcoming Cyber Espionage

The Stealthy ASBE Encrypted-Environment Thwarts Surveillance Attack Vectors

The recent exposure of the Carbanak Cybergang bank heist of $1 Billion[1], along with Anthem's loss of PII for roughly one-third of America's population[2] bares overwhelming evidence that industry and critical infrastructures are not prepared for the exacerbating sophistication of this new evolution of cybercriminal activity.

These intrusions implemented insidious strategy with a new complexity of tactics and methods, which cannot be overcome by merely encrypting the data, alone. Effective security now requires an integrative approach, which includes next-generation authentication and advanced encryption to aggressively defend against the relentless perseverance and pivot-ability of the cunning new criminal.

EMERGING CYBER ATTACK VECTORS

Acclaimed to have induced the most damaging fiscal, legal, and intelligence implications to date, these two compromises share a common method of assault. In each instance, the perpetrators infected system computers with advanced surveillance software… patiently hiding for months, while monitoring user actions to identify patterns and processes. This Intel enabled the attackers to simulate "authorized" credentials and/or "legitimate" procedures to steal data, validate bogus financial transactions, activate cash distributions from ATMs, and initiate other fraudulent action.

SEVERE SECURITY RAMIFICATIONS

The use of this comprehensive surveillance-APT raises disconcerting questions, including:

- *How does an entity protect against reconnaissance and sabotage, which masterfully counterfeits system environment procedures and employee access rights?*
- *How can authentication prevail over key-logger and video espionage?*
- *Is encrypting data futile against this new breed of attack?*

MERLINCRYPTION SOLUTION OVERVIEW

When an attacker can anticipate their target's every move, they can break through security, including the encrypted data to conquer from the inside out, Predictability makes it easy to gain access to the system, control encryption keys, conduct inside espionage, hide, spy, and steal.

MerlinCryption technology circumvents the criminal's ability to anticipate patterns and behaviors, through its unique application of "stochastic randomization" techniques, which are incorporated throughout its authentication, encryption, and patented random data generator. These three components are the foundation of a complete encryption security system, developed as a platform. The

Embedded Encryption Platform’s process also functions by this dynamic action, which leverages the variable results of its integral components. There are NO repeating patterns, behaviors, or outputs, which can be monitored, anticipated, and mimicked.

Criminals cannot predict the authentication factors, the encryption cyphertext, or the key size. Attackers cannot intercept or steal encryption keys, as there is no key transfer and no key storage.

NEXT-GENERATION AUTHENTICATION SUMMARY

Most authentication factors are based on something you know, something you have, and something you are. Carbanak and Anthem attackers imitated the authentication rights of employees or systems to gain access and control.

MerlinCryption has innovated a new 4th Category of authentication factors using information that is temporary and always unique. These factors are not deterministic, but are stochastic in nature.

Drawing from its “Temporary” Authentication Category, MerlinCryption has architected low-cost solutions, utilizing plug-in components, which work in tandem with unique human components. The authentication devices possess exponentially strong code to defeat the criminal’s ability to observe, monitor, and mirror factors for fraudulent access.

Additionally, MerlinCryption’s platform triggers Temporary and other factors, which dynamically act “under the hood." These unobservable factors can work both independently and symbiotically with employee access rights to thwart surveillance and insider espionage. The platform enables trusted programmers to change and automate factors in time variable intervals and in unique ways.

ADVANCED ENCRYPTION SYNOPSIS

Once inside the internal bank network, the Carbanak Cybergang identified and exploited repeating processes to crack the system and take control. Today’s encryption algorithms are static in nature, repeating processes over and over. Their behaviors are expected…patterns are anticipated

These encryptions use the same key and plaintext input, which always produced identical cyphertext output with every encryption instance. Results are always predictable.

MerlinCryption’s Anti-Statistic Block Encryption (ASBE) leverages dynamic algorithmic complexity and employs stochastic randomization in many aspects of its encryption process. Because all output is variable, there is no static behavior to monitor.

ASBE defeats Cryptanalysis and is anti-statistical. The algorithm *always* produces different cyphertext in *every* encryption instance, even when using the same key, the same password, and the same plaintext input,

ENCRYPTION KEY APPROACH OVERVIEW

The common approach to encryption key management, in itself creates security risks. Other encryption keys have a short length, which is fixed. Keys can be recognized by their size. The key is at risk of theft at every stage of the life cycle, particularly during transit and in storage depositories. This is increased through the use of certificate authorities.

MerlinCryption initiates a radically different approach to key generation and management. Keys and passwords are variable in length. Keys can be *any* size… from 2008 bits up to 2 GB…or any size in between. Because ASBE keys can change size with every encryption instance, they are exponentially more secure. ASBE Keys are layered with variable passwords, which also scale in length to 64KB. Hackers cannot identify, monitor, or predict patterns or behaviors.

ASBE Keys are created, used, and destroyed on the *EN*crypting end. Then recreated, used and destroyed on the *DE*crypting end. There is no key transfer, no key storage, no PKI, and no certificate authorities. Hackers are left with nothing to intercept or steal.

EMBEDDED ENCRYPTION PLATFORM SDK SNAPSHOT

The Carabank Cybergang successfully infiltrated their victim's administrative computers, as well as bank tellers, and other administrative personnel's activities to observe, anticipate, and impersonate. The Anthem hackers absconded with millions of records via a single employee's credentials.

MerlinCryption's Embedded Encryption Platform's highly sophisticated functionality is architected to allow the customer-organization to control all security. Only top trusted security programmers are authorized to dictate the platform's many dynamic variables or parameters, including size of keys and passwords, authentication factors, random data generator criteria, and what-when-where framework. *The platform's parameters are invisible to all other users of the system and therefore cannot be changed by malicious intent or in error*

The platform can be programmed to change authentication factors, keys, passwords, and other parameters mission-to-mission…hour-to-hour, minute-to-minute…or even transmission-to-transmission. The platform then automates ASBE encryption, authentication, and key generation "under the hood" with high performance.

The platform enables an ability to encrypt authentication, passwords, and data…then optionally encrypt all again. The result is layer, upon layer, upon layer of encrypted security.

GAME CHANGERS

- ASBE is more than twice as fast as AES
- Code footprint is negligible: Encryption Engine 22KB, Low Overhead Platform 55KB, Platform 200KB
- The platform is delivered in Software Developer Kits to further insulate customer security and control

CONCLUSIVE ACTION

Insidious attacks such as the Anthem and Carbanak Cybergang exploit predictable factors, anticipated behaviors, and expected patterns to penetrate and steal. MerlinCryption advanced technology uniquely applies stochastic randomization in the ASBE algorithm, authentication, key and password generation, and the Embedded Encryption Platform to create dynamic behaviors and output which countervail surreptitious attack.

The platform is architected for dynamic algorithmic flexibility and easily integrates into a wide variety of use cases, requiring encryption security, including system environments for financial, healthcare, military, SCADA, UAV, VoIP, Cloud, and data storage-only solutions for USB, SSD, and memory cards.

Additional benefits of MerlinCryption technology and the Embedded Encryption Platform SDK solution may be disclosed under NDA.

1. http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide
2. http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720