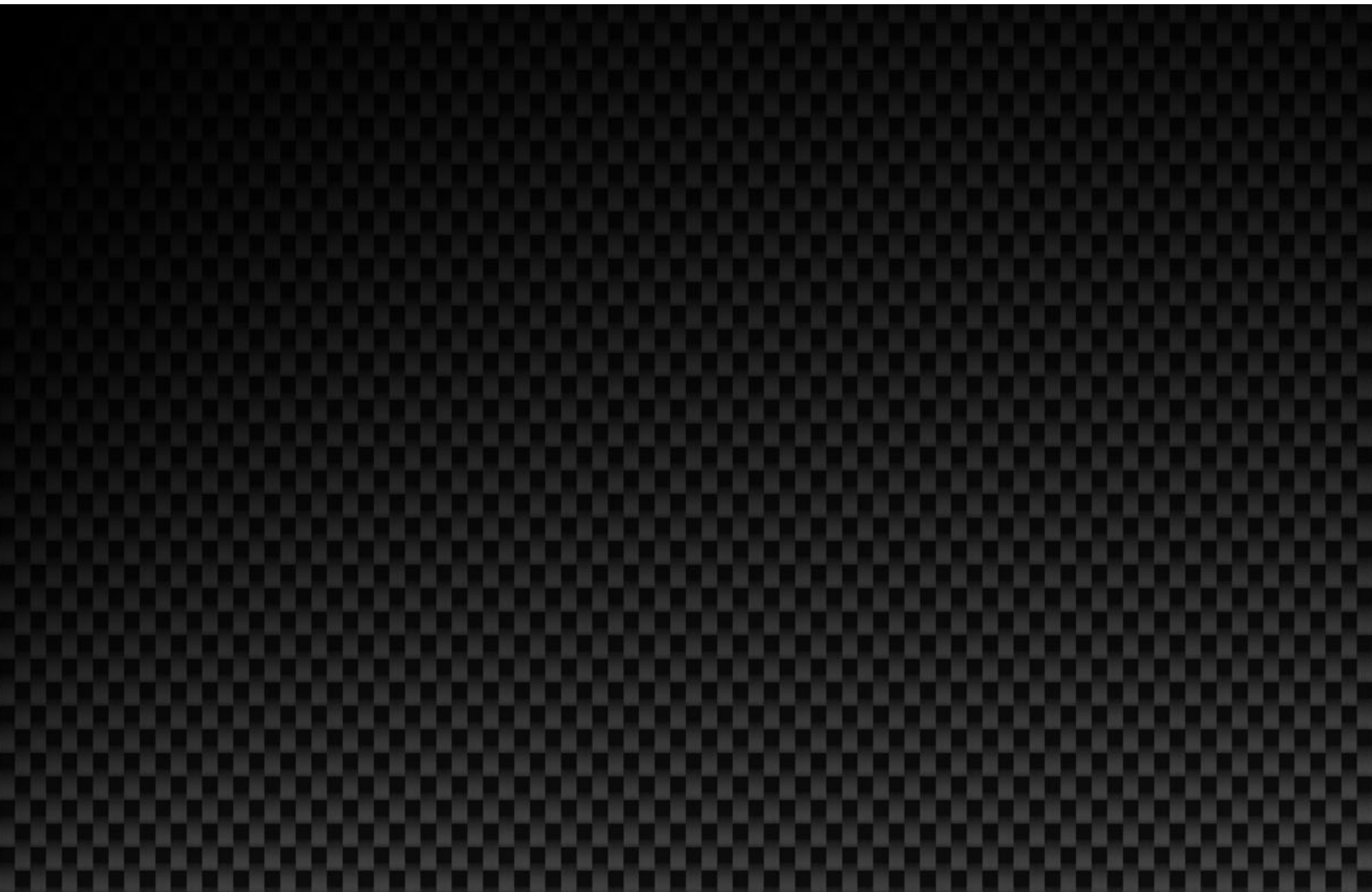
cybereason

Ransomware Decoded

Three Ways Ransomware Differs from Other Malware



RANSOMWARE IS HERE TO STAY

Ransomware attacks allow criminals to reap substantial profits with minimal effort compared to other attack methods. Spam campaigns, for instance, are nearly irrelevant while stealing credit card and bank account details requires an established criminal infrastructure to monetize this information.

With ransomware, a small group of attackers can use Bitcoin to quickly and easily make money. Bitcoin is the de facto currency for ransomware attacks. The digital currency provides attackers with the perfect cover. Bitcoin transactions are anonymous and, unlike traditional bank transactions, are irrevocable once they're complete.

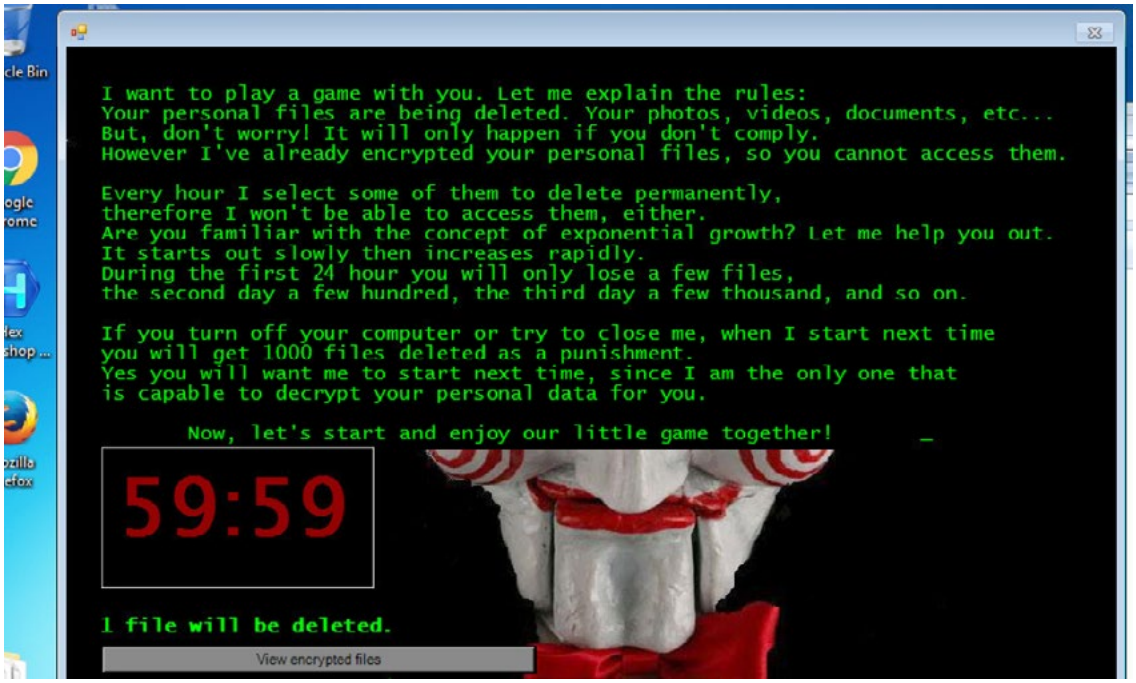
In fact, there's been a spike in ransomware attacks since Bitcoin usage took off in 2013, showing that criminals have embraced this threat. That year, at least five ransomware strains were identified, including CryptoLocker, which is the first strain that required payment in Bitcoin. By comparison, approximately 15 strains were identified in just the first quarter of 2016, including KeRanger, the first one to target computers running Mac OS X.

HOW RANSOMWARE DIFFERS FROM OTHER MALWARE

Malicious code can be detected by either looking at what it is or what it does. The first method is the simpler and older of the two and uses the code's static properties like its binary hash, contained binary sequences and strings, name, entropy or imported functions.

However, ransomware-on-demand services and self-modifying code easily generate completely new code with the same functionality, making this detection method obsolete. The ransomware distribution system described by Cybereason in its Operation Kofer research is just one example of an attack where each victim was infected with a unique ransomware binary. In addition, ransomware is the preferred payload for drive-by download and malvertising campaigns. Both of these attacks infect victims without their knowledge and, unfortunately, spam filters and sandbox email scanning systems cannot prevent them.

The only realistic way to detect ransomware is by looking at what it does, the heuristic behavioral approach. But there's a catch—ransomware has a few key differences that make it stand out from other malicious programs.



The Jigsaw ransomware letting us know it's here

RANSOMWARE IS NOT SUBTLE

Most malware silently persists in the network, carefully surveying the network surroundings, awaiting instructions or the right opportunity to attack. These programs mask their actions to evade detection and attempt to gain elevated privileges. Ransomware, on the other hand, is nasty stuff and wants to be discovered. As soon as the program starts encrypting files, it reveals itself to the victim and demands a hefty ransom, many times along with various threats.

Cybereason's research into ransomware strains shows that while some are very sophisticated, many are crude and poorly written. But just like an improvised weapon, the less refined strains are easy to produce and can be extremely effective. A piece of malicious code that promotes its existence upends the way most traditional anti-malware products work. You may think that lacking intricate malicious mechanisms makes ransomware easier to detect. But often times malicious behaviors and techniques are malware's weak spots and make these programs stand out to defenders

RANSOMWARE DOESN'T NEED TO BE ACCURATE

Banking Trojans steal credit card numbers and bank account details by carefully extracting them from specific locations in the browser when it accesses specific domains. Ransomware, on the other hand, just wants to cause as much damage as possible. It doesn't need to encrypt all of your files to be successful, it just needs to scramble enough important ones.

Ransomware grabs and encrypts anything: quarterly revenue spreadsheets, Word documents, PowerPoint presentations, generic README files, family photos. And the list goes on. Ransomware fires in all directions and hopes to hit something important. This lack of specificity makes ransomware more difficult to detect. You can't concentrate on defending only certain locations or applications. You have to monitor everything, all the time.

RANSOMWARE IS ALARMINGLY QUICK

Ransomware takes between five and 20 minutes to encrypt every relevant file on the average hard drive (depending on the speed of the machine and the number of files). That means that even the slowest, single-threaded ransomware can encrypt several potentially important files in seconds. Since ransomware works quickly, detection and response time is of the utmost importance, which may be problematic for certain behavioral-detection solutions. Unlike detection based on what the code is, detecting what the code does is prone to false positives and requires collecting additional evidence before a verdict is reached.

Every ransomware program goes over files, chooses the ones that look interesting, encrypts them and destroys the originals. You know what else does this? Compression software, legitimate encryption applications and backup and cloud-sync solutions in addition to many more programs. The same behavior is exhibited even if you manually compress a directory with a password and then delete it. Since ransomware encrypts any file anywhere on a computer, it's extremely difficult to distinguish a legitimate file activity from a malicious one. While every encrypted file increases the likelihood that the ransomware will be detected, each encrypted file equals another important piece of information lost. Every second counts when ransomware starts encrypting files.

Even the slowest, single-threaded ransomware can encrypt several potentially important files in seconds.

PROTECT YOUR DATA FROM BEING HELD HOSTAGE

Cybereason researched more than 40 ransomware strains, including Locky, Cryptowall, TeslaCrypt, Jigsaw and Cerber and identified the behavioral patterns that distinguish ransomware from legitimate applications. Whether a criminal group or nation created the program, all ransomware functions the same way and encrypts as many files as possible. These programs can't determine what files are important so they encrypt everything based on file extensions.

RansomFree, Cybereason's anti-ransomware tool, takes ransomware's behavior into consideration. By putting multiple deception methods in place, RansomFree detects ransomware as soon as encryption occurs either on a computer or network drive. Once encryption is detected, RansomFree suspends it, displays a pop-up that warns users their files are at risk and enables them to stop the attack.

RansomFree protects against local encryption as well as the encryption of files on network or shared drives. The encryption of shared files is among the doomsday scenarios an organization can imagine. It takes only one employee on the network to execute ransomware and affect the entire company.

RansomFree catches stand-alone ransomware programs as well as fileless ransomware. Stand-alone ransomware uses vulnerabilities in applications, like buggy Flash code, while fileless ransomware abuses legitimate Windows tools, like the PowerShell scripting language or JavaScript, to carry out its malicious intentions.

RansomFree, Cybereason's anti-ransomware tool, protects against local encryption, the encryption of files on network or shared drives, and catches stand-alone ransomware programs as well as fileless ransomware.

RANSOMWARE DOESN'T DISCRIMINATE

Attackers know people place a premium on certain files. Businesses have spreadsheets loaded with sales data while everyone treasures photos of family vacations, baby's first steps, etc. And while backing up files is critically important, this step may not protect a person or an organization from ransomware if a network drive becomes infected. And since ransomware has proven lucrative for adversaries, they're not likely to remove this threat from their toolkit any time soon. Using RansomFree ensures that valuable data, whether it's a person's wedding photos or a company's product roadmaps, won't be held hostage by cyber criminals.

See how RansomFree by Cybereason keeps your data safe from never-before-seen ransomware.

cybereason

Founded by members of the Israeli intelligence agency's elite cyber security Unit 8200, Cybereason mirrors the founders' expertise in managing some of the world's most complex hacking operations. Cybereason developed the world's only military-grade, real-time detection and response platform and has a proven track record of protecting Fortune 1,000 enterprises globally. The company has received many awards and accolades since its founding.

Cybereason Inc. is privately held and headquartered in Boston with offices in Tel Aviv and Tokyo.