cybereason

Lab Analysis

Operation Kofer: Mutating Ransomware Enters the Fray

By: Uri Sternfeld, Senior Security Researcher

Contents

Cybereason Labs discovered a massive operation used for the distribution of automatically-generated ransomware variants.

Cybereason researchers discovered numerous ransomware variants last week that share the same general packaging and delivery techniques but incorporate random variables that help them evade static-signature or hash-based detection.

The similarity of the variants leads us to believe that they were all created by the same group, which automatically generates a new variant for every new target to avoid signature-based detection. They also include mechanisms that help them evade detection by sandboxes and other dynamic detection tools, as well as embellishments that attempt to fool malware researchers.

Operation Kofer appears to be the first “drive-by” ransomware operation to incorporate an APT/nation-state level of complexity, making it an increasing threat for organizations. We believe Operation Kofer to have a European-wide presence, as we detected variants that target Spanish, Polish, Swiss and Turkish targets, among others.

Key Findings

Cybereason Lab researchers examined several different samples of ransomware sourced from different victims across the world. Each of these samples has a different hash and unique characteristics, but also several shared details that allowed us to make a connection between them. We believe that they were all created by the same operational group or R&D team using an automated algorithm to “mix and match” together different components, forming a completely new variation each time (see table below for details). These similarities tie the otherwise very different samples together into a single operation. All of the variants were found and compiled during the last couple of weeks, while new ones are generated every few days, or even hours.

Similarities and Differences Among Kofer Variants

Delivery techniques:

- All of the analyzed Kofer variants presented a fake icon, most often that of a PDF document.
- All variants used a bogus file name meant to deceive the recipient into double-clicking the file. This suggests that the main method of delivery is probably mass email campaigns that target specific organizations or countries.

Anti-detection techniques:

- The ransomware payload is stored encrypted as a benign-looking resource inside the PE, prefixed by a 1K unrelated header taken from various sources (we identified several types of such headers, which allowed us to incriminate other variants of the malware). This is done to evade detection during casual examination of the file's contents.
- Many other "junk" resources (dialog boxes, bitmaps, strings, etc.) are also added at random from a given set to make the file look even more benign.
- The package executes itself as a child process, a method used to evade detection by some sandboxes and other dynamic detection solutions as they might only track the original process.
- Some variants check whether they are being executed inside a virtual machine, and if so, refuse to run.
- Some variants inject themselves into a newly spawned explorer.exe process.

- For persistence, some variants copy themselves to a constant, benign-looking path, while others generate a path at random. These paths are then added to various autorun locations in the registry.
- Some variants delete the original executable after running, while others do not.

Payload:

- At least two ransomware variants were detected - CryptoWall 3.0 and Crypt0L0cker - and others are also suspected to be a part of the operation.
- Some of the variants use TOR for C&C communication.
- Some variants destroy Shadow Copies on the local machine to prevent any possibility of file recovery

Detection of Kofer Variants

As the Kofer operation quickly creates new, mutated versions of ransomware, one cannot rely on detection by binary hashes, string identification, API calls or sandbox behavior. Also, network-only tools that do not have an endpoint element will most probably fail to detect malicious TOR-based activity, as it's impossible to distinguish legitimate TOR processes from the malware.

The best detection approach would combine the following:

1. **Endpoint visibility:** One must have full visibility to all endpoint activities to spot a these executable files based on common heuristic characteristics.
2. **Behavioral detection:** Continuously monitor behavior on the endpoint and constantly compare it to all other behavior on all endpoints across the organization to spot suspicious abnormal behavior.
3. **Instant Recognition:** It is crucial to detect ransomware quickly to stop it from impacting a large portion of the organization's endpoints. Therefore, it is key to have real-time visibility of endpoint behavior.

Mitigation Suggestions

1. Network shares pose a huge risk in cases of ransomware as a single endpoint infection can cause significant data loss. To help protect against the data loss, administrators can set up a volume Shadow Copies to update frequently. This can provide a highly reliable short-term online file backup solution.
2. Frequent offline/cold backups of your data are absolutely essential. Cloud backup services with local clients (e.g. Dropbox, Google Drive, etc.) are easily defeated by some ransomware.
3. Almost all observed variants look for the file “C:\myapp.exe,” and if a file with this name is present - refuse to run. This can be an effective method of preventing infection (the file just needs to exists, and is not required to be a real executable file - any file will do), though this behavior may be modified in the future.

Bottom Line

The new “drive-by” attacks are leveling up and becoming APT-grade in their sophistication, as well as their ability to mutate and evade detection. Their continual spread clearly presents the need for an advanced detection approach.

Comparison of Kofer Variants

Colors represent similar components in variant distributions.

MD5	Compliation Date	Icon	File name(s)	Internal Languages	Payload "Mask"	Payload
8F9916F20E575957701AA88AE303DFFC	06/14/2015	CSV document	cacde0e5.exe 79773e5b.exe	N/A	Compiled .obj	CryptoWall 3.0
F63C25E11D822EFBC336A9E1D6FC1E03	06/16/2015	Adobe PDF document	F-VAT_czerwiec.pdf.scr ("June" in Polish) windykacja_kruk_sa.pdf.scr ("Bill" in Polish)	N/A	Compiled .obj	?
5DCBE0267C24F5AD50277A60302F5380	06/22/2015	Wall-E Icon	ipgya.exe	N/A	Compiled .obj	?
C3BCA74ABC8E17AC6C47D1004426664A	06/23/2015	Adobe PDF document	my_resume_pdf_id-1851-2447-293.scr	N/A	Apache JAR	CryptoWall 3.0
E576AE9D7785CFC351E843A709B709DB	06/27/2015	Adobe PDF document	turkcell_192189779.exe Pacchetto_847512.exe ("Package" in Spanish)	N/A	Apache JAR	?
067FAF4A6C548AD65A80B2725BBABDAD	07/01/2015	Adobe PDF document	my_resume_rpd_id-4547-4657-293.scr Puzzle.exe	German	VM image	CryptoWall 3.0
2F4110CB60316B42A236B9B28792D2D6	07/02/2015	Adobe PDF document	Bolletta_125478.exe ("Bill" in Spanish)	N/A	VM image	Crypt0L0cker
DA1E4E22F1F7D3238E2CCC01388C2B21	07/04/2015	Adobe PDF document	Bolletta_452147.exe ("Bill" in Spanish)	N/A	VM image	Crypt0L0cker
EF76C389E20544FC13FB681FB4892F67	07/05/2015	Adobe PDF document	my_resume_pdf_id-4637-7957-4663.scr MazeByWen.exe	French	VM image	CryptoWall 3.0
0612DA36AB36230731A510CA96BF95D1	07/05/2015	Adobe PDF document	Bolletta_185746.exe ("Bill" in Spanish) MazeByWen.exe	French	VM image	Crypt0L0cker

1 Broadway, 15th Floor
Cambridge, MA 02145 USA
www.cybereason.com

About Cybereason

Cybereason was founded in 2012 by a team of ex-military cybersecurity experts to revolutionize detection and response to cyber attacks. The Cybereason Malop Hunting Engine identifies signature and non-signature based attacks using big data, behavioral analytics, and machine learning. The Incident Response console provides security teams with an at-your-fingertip view of the complete attack story, including the attack's timeline, root cause, adversarial activity and tools, inbound and outbound communication used by the hackers, as well as affected endpoints and users. This eliminates the need for manual investigation and radically reduces response time for security teams. The platform is available as an on premise solution or a cloud-based service. Cybereason is privately held and headquartered in Boston, MA with offices in Tel Aviv, Israel.