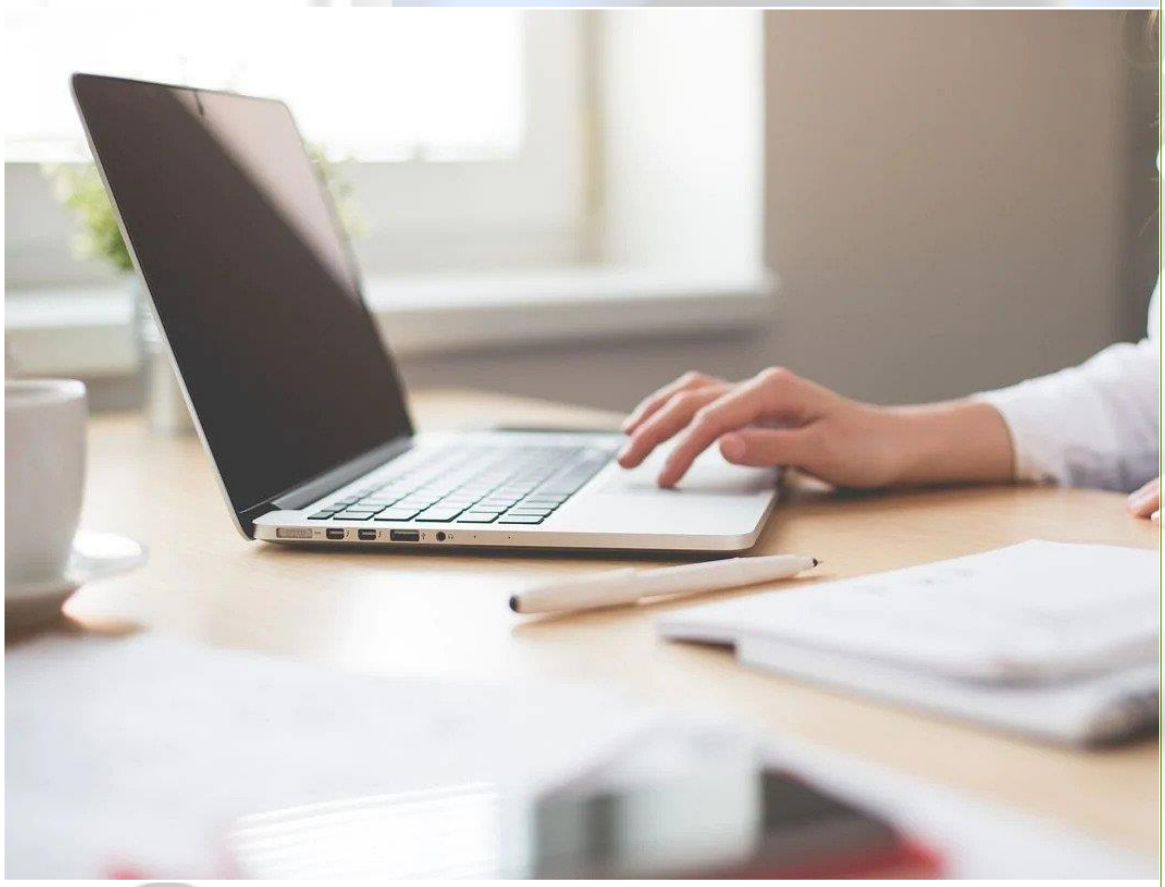
CRYPTUS CYBER
SECURITY PVT. LTD.

Module:-

Analysis On Ransomwares

By-Sahil Thakur



Ransomware – Mechanisms and Protection

Ransomware is one of the fastest-growing threats in the cybersecurity landscape. Nowadays, it feels like a day doesn't go by without news of another major outbreak of ransomware somewhere in the world.

At the time of writing (24 October 2017), a new strain of ransomware known as Bad Rabbit has just attacked organizations in Russia and Ukraine. As reported by Carbon Black, Bad Rabbit uses the infamous EternalBlue exploit that affects Windows systems. Despite being patched by Microsoft in the middle of 2017, this exploit is still effective since many users have failed to update their Windows computers.

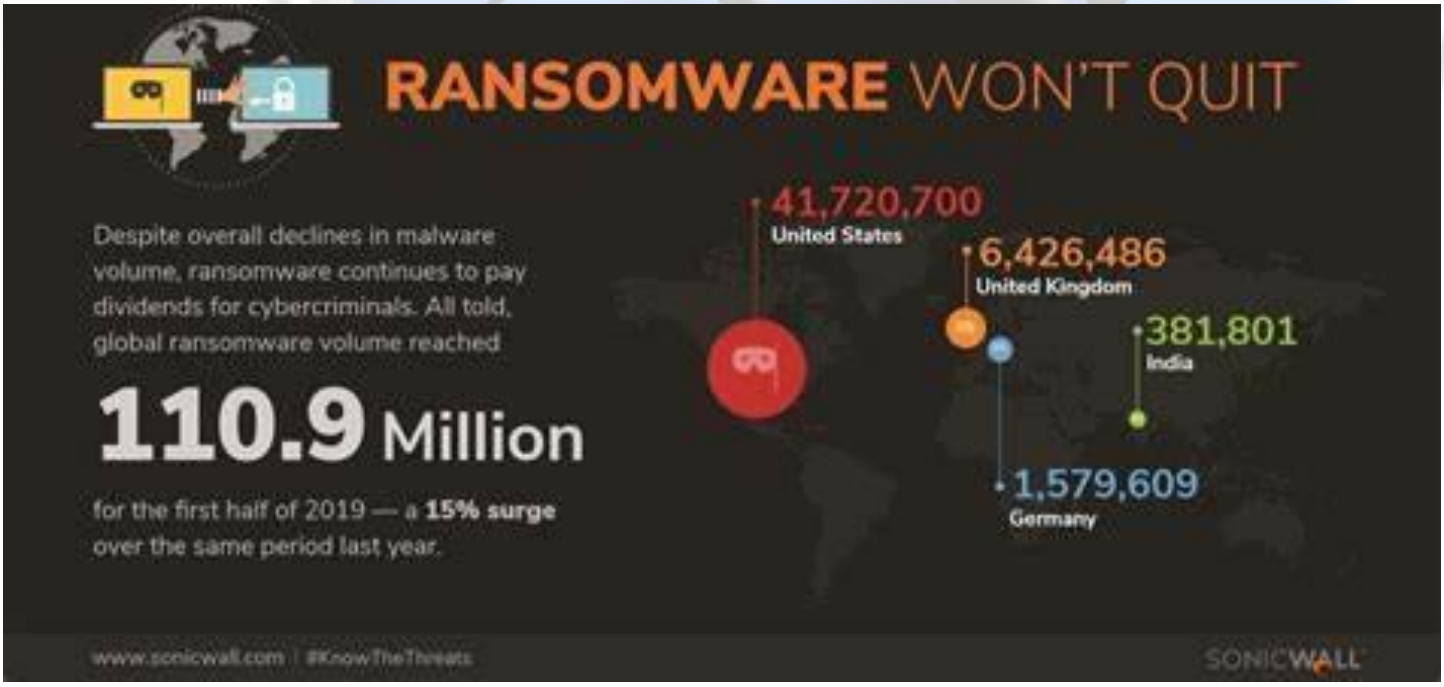
Quantifying the prevalence of ransomware

Windows is not the only operating system to be affected by ransomware outbreaks, however. According to statistic from Kaspersky Lab, 218,265 types of ransomwares targeting mobile devices were detected in Q1 2017. Over that same quarter, the share of Trojan ransomware among all mobile threats increased 3.5 times compared to the previous quarter (from 4.64% to 16.42%).

Over the same period, 240,799 mobile users were affected by Trojan ransomware. Every major system, including macOS and Linux, is susceptible to an attack.

According to an interagency publication released by the US government, the average number of daily ransomware attacks increased by 300% between 2015 and 2016 (1,000 attacks daily in 2015 vs. 4,000 attacks daily in 2016). Cybersecurity Ventures reports that the yearly global cost of ransomware is projected to reach $5 billion by the end of 2017, a 15-fold increase compared to 2015.

The financial effectiveness of ransomware had led to a booming black market for ready-to-use products. Research on the dark web economy conducted by Carbon Black shows a staggering 2,502% increase in ransomware sales on the black market in 2017 as compared to 2016. This goes to show that ransomware that can easily be used without any special technical knowledge is available for purchase to anyone willing to pay.



Developing a ransomware protection solution

In the current environment, the demand for systems that are be able to protect against ransomware has also increased. However, actually developing solutions that are capable of effectively dealing with never-before-seen threats is extremely challenging. Regular signature-based antivirus software is ill-fitted to tackle zero-day attacks.

Next-generation threat hunting solutions are required. The endpoint security market is expanding developing two strategies: **advanced detection** (typically, such solutions are based on event-driven behavior analytics approach, e.g. Carbon Black platform) and **advanced prevention** (focusing on blocking system penetration attempts whenever started, see Harpoon Security).

Participating in numerous cybersecurity projects over the years, we've developed a range of technologies for our clients including ones that successfully detect and prevent zero-day attacks. We've created solutions for in-depth system monitoring at all levels, including for detecting hidden processes, all file operations, integrity violations, and various hooks, which is exactly what's required to successfully detect a novel ransomware infection.

In this article, we'll share our experience and talk about the definition and popular types of ransomware. We'll also show how you can use system monitoring coupled with behavior analytics to detect attacks by new, never-before-seen strains and discuss advanced prevention of zero-day attacks on the earliest stage.

Definition of ransomware

Ransomware is a type of malicious software designed to extract a ransom from the user of an infected system. Several types of it exist and are distinguished by the different tactics they use for extracting the ransom:

- **System lockers** block the user from accessing the operating system until a ransom is paid.
- **Application lockers** block the user from accessing certain software or functionality (usually a web browser or specific websites) until a ransom is paid.
- **Data encrypting ransomware** encrypts data on the targeted system until a ransom is paid.
- **Fake data encryption ransomware** simply deletes all data while trying to convince the user that the data has been encrypted and trying to extort a ransom to unlock it.

Origin of ransomware

The concept of ransomware first appeared in the late 80s with the AIDS Trojan, which used encryption techniques to lock users out of their systems and files. Similar malware continued to re-emerge all throughout the 90s and early 2000s. However, weak cryptographic algorithms and the difficulty of anonymously extorting money limited the effectiveness and popularity of this method.

Things changed dramatically with the advent of Bitcoin – cryptocurrency that allows for near-anonymous transactions. Bitcoin was first used as a means to pay ransoms in 2013 by **CryptoLocker**, a new strain of ransomware that was spread through infected email attachments. CryptoLocker targeted Windows systems and encrypted all files of certain types using asymmetrical cryptography (a pair of public and private keys) while demanding a payment in Bitcoin equivalent to $400.

CryptoLocker proved financially successful, producing an estimated $3 million in ransom. This led to the explosion of ransomware, with many perpetrators copying CryptoLocker's design while improving it and expanding on it, which eventually led to the situation we have today which is characterized by an explosion of black market offers and even the advent of ransomware as a service.

Notable strands of ransomware

Beyond CryptoLocker and its numerous clones, other notable types of ransomwares include:

Cryptowall. Another extremely successful ransomware that first appeared in 2014, the Cryptowall strain affected nearly 1000 victims throughout its first year, costing them up to $18 million in damages and ransom. One of the key features of this strain is a trick it uses to avoid detection: the use of an actual digital signature. Cryptowall also creates fake explorer.exe and svchost.exe processes to mask its presence in the system. The typical amount of ransom asked by Cryptowall ranged from $700 to $1400 depending on the time elapsed from the moment of encryption. Cryptowall was distributed by infected email attachments as well as by malicious ad campaigns (a delivery method otherwise known as *malvertising*).

Locky. Similar to CryptoLocker but far more advanced in terms of encryption and obfuscation methods, Locky first appeared in 2016 and was delivered by malicious email attachments. With the use of complex encryption algorithms with server-side key generation that makes manual decryption impossible, Locky can encrypt files on all available drives including fixed, removable, and network.

Wannacry. This extremely prominent ransomware infected more than 230,000 endpoints in May 2017. It brought down almost all of the National Health Service in the UK.

Wannacry famously used the EternalBlue exploit, mentioned above, in order to strike vulnerable Windows systems. Although a patch for this exploit was issued prior to the Wannacry attack, many organizations failed to update their systems, making them susceptible.

Petya. This ransomware was first discovered in 2016. Petya uses an encryption technique to fully block the user out of the system by infecting the Windows Master Boot Record and subsequently encrypting the file system table of the main Windows drive. The original Petya used email attachments to spread, although a new strain called NotPetya that emerged in 2017 adopted the use of the EternalBlue exploit.

Typical ransomware behavior

Although numerous strains of ransomware exist, each using a different delivery method and different encryption algorithm, there are certain patterns of behavior that can be attributed to the majority of different strains. Such behavior includes:

- **Persistent payload** – Like a majority of malware, ransomware needs a way to ensure that the attack can be continued and completed even if the target endpoint is rebooted. Thus, the majority of ransomware uses built-in operating system functionality to ensure that it will start automatically after reboot. For Windows systems, it can place itself in the startup folder, modify the registry, create a scheduled task to run automatically, and so on.

- **Disabling system restore functionality** – Ransomware usually tries to disable all built-in system features that allow users to restore

altered files or roll back the system to a previous state. For Windows, it usually disables the system restore service and deletes shadow copies in order to block the user from at least partially restoring encrypted data and access to the system.

- **Environment mapping** – Before initiating an attack, ransomware usually maps the environment of the system it runs on. This can have several applications. First of all, it allows ransomware to determine the target location and language. Certain strands use this information to avoid targeting endpoints located in certain countries. For example, the Cerber ransomware is designed not to initiate an attack if it detects that a target system uses the Russian language. Environment mapping can also be used to detect valuable files that can be targeted for encryption as well as security measures that can be bypassed. Some ransomware strains also use environmental mapping for protection, by detecting whether they're running on a real machine or on a virtual machine. When a virtual machine is detected, the ransomware shuts down to prevent security specialists from studying its behavior.
- **Network usage** – Ransomware can use existing network connections to send encryption keys to the remote server. Sometimes, additional payload files are also downloaded via the network – something that is often seen in targeted ransomware, or the type designed to take advantage of a particular exploit. To preserve anonymity, perpetrators often register randomly generated domain names with anonymous top-level domains.

- **Privilege escalation** – Sometimes, in order to initiate an attack and cover the tracks, ransomware may require administrative permissions

(to overwrite the Master Boot Record, for instance) that are not available to the current user. Thus, various methods can be used to escalate the privilege level.

- **Mass file operations** – When encrypting data, ransomware tends to move and delete original files while at the same time generating new ones. It also often renames files en masse, usually adding an extension to the original filename.
- **Ransom notes** – Ransomware typically uses ransom notes to communicate ransom demands to victims. Some strains opt for text-based notes, while others use images. Ransom notes are located within the malware files and can be used to identify it.

Additionally, ransomware often uses all of the tactics employed by a typical Trojan or a virus in order to go undetected. Such tactics include running under fake system processes, executing from system directories, and using system executable names.

A behavior-based approach to ransomware detection

So, how to prevent a ransomware attack and how we can detect previously unknown threats?

Traditional malware detection software uses statistical and signature-based approaches. Both of these approaches rely on existing datasets containing signatures and known information about detected malware that each new file can be compared against. While this approach works great for detecting known malware, it's often unable to detect novel threats as well as malware that uses code obfuscation extensively.

Considering the speed with which new strains of ransomware are being developed, the effectiveness of signature-based and statistical-based methods in stopping ransomware drops by the minute.

A new approach that can detect both known and new types of ransomware combines in-depth system monitoring and machine learning for behavior-based detection.

A system can be monitored for the typical ransomware behavior described above. When such behavior is detected, the associated file can be immediately quarantined.

It's worth noting that detecting a single behavioral indicator does not allow you to reliably identify malware. In order to avoid false positives and false negatives, you need to identify several behavioral indicators and establish a connection among them. This means that events need to be analyzed not separately, but rather in streams in order to get the proper context for each event.

A quick thought here is the more enhanced a behavior analysis algorithm is the better solution works, but it's not quite that simple.

Potential challenges

A behavior-based approach to ransomware detection for detecting unknown variants still isn't perfect. There are certain issues that can arise and need to be tackled individually at the early stages of planning and developing anti-ransomware software:

- **Critical performance requirements** – A behavior-based approach requires real-time system monitoring and analysis, which often proves quite resource-intensive. For a quick removal and to limit the potential damage from ransomware as much as possible, it needs to be detected in real time, with critical time typically equaling 1-3 minutes. Complex analysis and event correlation algorithms can simply be late with delivering an alert notification. Behavior analytics system engineers are always balancing between a substantial amount of optimization at all stages of the pipeline and designing smart combinations of simpler analysis algorithms.
- **Establishing an effective baseline** – Behavior-based systems work by analyzing the current stream of events and comparing it to an established baseline for normal system behavior. If this baseline is chosen incorrectly, it can lead to a high number of false positives or false negatives. The biggest challenge in this regard is gathering the initial dataset. Beyond that, the system needs to study the behavior of certain malware types in order to reliably detect them. Collecting a variety of existing ransomware examples can also prove quite a challenge.
- **Susceptibility to behavioral obfuscation** – Behavioral obfuscation, similar to code obfuscation, is designed to conceal the behavior of malware by creating a certain amount of behavioral noise, making the malware undetectable by behavior-based detection solutions. Very few types of ransomwares currently use behavior obfuscation, but as it becomes more popular it may prove to be a serious challenge in the future.

Alternative approach: early blocking

An alternative strategy focuses on the moment ransomware and other malware penetrate a working system.

The solution monitors and blocks malicious in-memory injections such as reflective DLLs or process injections without full attack pattern inspection, whatever simple or complex it is. Thus, it naturally avoids issues with time-consuming event correlation, "behavior noise", or system-wide baselining.

This approach also has its challenges, such as stable low-level system monitoring, reliable discerning of legitimate and malicious resource usage, comprehensive coverage of all possible injection landscape, staying non-intrusive for the legitimate activity. But with all the questions answered, this threat prevention software proves to be effective cutting both known and unknown attacks at their starting point.