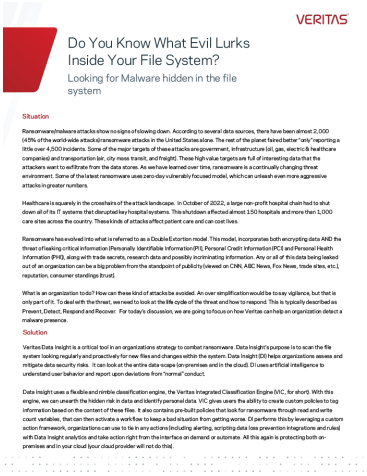
VERITAS

Do You Know What Evil Lurks Inside Your File System?

Looking for Malware hidden in the file system

Situation

Ransomware/malware attacks show no signs of slowing down. According to several data sources, there have been almost 2,000 (45% of the world-wide attack) ransomware attacks in the United States alone. The rest of the planet faired better "only" reporting a little over 4,500 incidents. Some of the major targets of these attacks are government, infrastructure (oil, gas, electric) & healthcare companies) and transportation (air, city mass transit, and freight). These high value targets are full of interesting data that the attackers want to exfiltrate from the data stores. As we have learned over time, ransomware is a continually changing threat environment. Some of the latest ransomware uses zero-day vulnerably focused model, which can unleash even more aggressive attacks in greater numbers.

Healthcare is squarely in the crosshairs of the attack landscape. In October of 2022, a large non-profit hospital chain had to shut down all of its IT systems that disrupted key hospital systems. This shutdown affected almost 150 hospitals and more than 1,000 care sites across the country. These kinds of attacks affect patient care and can cost lives.

Ransomware has evolved into what is referred to as a Double Extortion model. This model, incorporates both encrypting data AND the threat of leaking critical information (Personally Identifiable Information(PII), Personal Credit Information (PCI) and Personal Health Information (PHI)), along with trade secrets, research data and possibly incriminating information. Any or all of this data being leaked out of an organization can be a big problem from the standpoint of publicity (viewed on CNN, ABC News, Fox News, trade sites, etc.), reputation, consumer standings (trust).

What is an organization to do? How can these kind of attacks be avoided. An over simplification would be to say vigilance, but that is only part of it. To deal with the threat, we need to look at the life cycle of the threat and how to respond. This is typically described as Prevent, Detect, Respond and Recover. For today's discussion, we are going to focus on how Veritas can help an organization detect a malware presence.

Solution

Veritas Data Insight is a critical tool in an organizations strategy to combat ransomware. Data Insight's purpose is to scan the file system looking regularly and proactively for new files and changes within the system. Data Insight (DI) helps organizations assess and mitigate data security risks. It can look at the entire data scope (on-premises and in the cloud). DI uses artificial intelligence to understand user behavior and report upon deviations from "normal" conduct.

Data Insight uses a flexible and nimble classification engine, the Veritas Integrated Classification Engine (VIC, for short). With this engine, we can unearth the hidden risk in data and identify personal data. VIC gives users the ability to create custom policies to tag information based on the content of these files. It also contains pre-built policies that look for ransomware through read and write count variables, that can then activate a workflow to keep a bad situation from getting worse. DI performs this by leveraging a custom action Framework, organizations can use to tie in any actions (including alerting, scripting data loss prevention integrations and rules) with Data Insight analytics and take action right from the interface on demand or automate. All this again is protecting both on-premises and in your cloud (your cloud provider will not do this).

Do You Know What Evil Lurks Inside Your File System?

Looking for Malware hidden in the file system

Thank you for downloading this Veritas solution brief. Carahsoft is the market vendor for Veritas solutions available via the GSA, ITES-SW2, NASA SEWP V, and other contract vehicles.

To learn how to take the next step toward acquiring Veritas' solutions, please check out the following resources and information:

For additional resources:
carah.io/VeritasResources

For upcoming events:
carah.io/VeritasEvents

For additional Veritas solutions:
carah.io/VeritasSolutions

For additional Veritas 360 Defense solutions:
carah.io/360Defense

To set up a meeting:
Veritas@carahsoft.com
(888)-662-2724

To purchase, check out the contract vehicles available for procurement:
carah.io/VeritasContracts

For more information, contact Carahsoft or our reseller partners:
Veritas@carahsoft.com | (888)-662-2724

Do You Know What Evil Lurks Inside Your File System?

Looking for Malware hidden in the file system

Situation

Ransomware/malware attacks show no signs of slowing down. According to several data sources, there have been almost 2,000 (45% of the world-wide attacks) ransomware attacks in the United States alone. The rest of the planet faired better "only" reporting a little over 4,500 incidents. Some of the major targets of these attacks are government, infrastructure (oil, gas, electric & healthcare companies) and transportation (air, city mass transit, and freight). These high value targets are full of interesting data that the attackers want to exfiltrate from the data stores. As we have learned over time, ransomware is a continually changing threat environment. Some of the latest ransomware uses zero-day vulnerably focused model, which can unleash even more aggressive attacks in greater numbers.

Healthcare is squarely in the crosshairs of the attack landscape. In October of 2022, a large non-profit hospital chain had to shut down all of its IT systems that disrupted key hospital systems. This shutdown affected almost 150 hospitals and more than 1,000 care sites across the country. These kinds of attacks affect patient care and can cost lives.

Ransomware has evolved into what is referred to as a Double Extortion model. This model, incorporates both encrypting data AND the threat of leaking critical information (Personally Identifiable Information (PII), Personal Credit Information (PCI) and Personal Health Information (PHI)), along with trade secrets, research data and possibly incriminating information. Any or all of this data being leaked out of an organization can be a big problem from the standpoint of publicity (viewed on CNN, ABC News, Fox News, trade sites, etc.), reputation, consumer standings (trust).

What is an organization to do? How can these kind of attacks be avoided. An over simplification would be to say vigilance, but that is only part of it. To deal with the threat, we need to look at the **life cycle** of the threat and how to respond. This is typically described as Prevent, Detect, Respond and Recover. For today's discussion, we are going to focus on how Veritas can help an organization detect a malware presence.

Solution

Veritas Data Insight is a critical tool in an organizations strategy to combat ransomware. Data Insight's purpose is to scan the file system looking regularly and proactively for new files and changes within the system. Data Insight (DI) helps organizations assess and mitigate data security risks. It can look at the entire data-scape (on-premises and in the **c**loud). DI uses artificial intelligence to understand user behavior and report upon deviations from "normal" conduct.

Data Insight uses a flexible and nimble classification engine, the Veritas Integrated Classification Engine (VIC, for short). With this engine, we can unearth the hidden risk in data and identify personal data. VIC gives users the ability to create custom policies to tag information based on the content of these files. It also contains pre-built policies that look for ransomware through read and write count variables, that can then activate a workflow to keep a bad situation from getting worse. DI performs this by leveraging a custom action framework, organizations can use to tie in any actions (including alerting, scripting data loss prevention integrations and rules) with Data Insight analytics and take action right from the interface on demand or automate. All this again is protecting both on-premises and in your cloud (your cloud provider will not do this).

The AI in DI can be used to detect anomalous behavior, what IF situations. What if thousands of files are being encrypted? What if DI detects a series of ransomware file extensions (locky, MERRY, zzz, r5a, etc.) that may or may not be active, but lying in wait within the system. Obviously doing nothing is not an option, so, what does an organization do? Using Data Insight's flexible actions framework, administrators will have a work area that simplifies remediation efforts by automating monitoring, migration, and protection of data. Administrators are armed with single-click access to classify and interrogate—all from Data Insight's easy-to-use workbench.

Conclusion

Veritas Data Insight helps enterprises proactively assess and mitigate unstructured and sensitive data security risks. With Data Insight, you can classify sensitive data in a hybrid cloud environment and arm your operations team with the key knowledge needed to identify security threats and prepare compliance audits more efficiently. Combining data visibility, context and analytics across your whole infrastructure allows IT to gain relevant knowledge to improve data governance and resolve security, compliance, insider and cyber threats quickly and conclusively.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact