Eliminating the Embedded Malware Threat at the Binary Level

Attack methods that evade enterprise security controls are understandably favored among cybercriminals, and the growing trend toward embedding malware in documents is evidence of the difficulty of detecting this activity.

In April 2019, Jonathan Tanner, senior security researcher at Barracuda Networks, reported that of the 300,000 malware-infected files examined in the previous 12-month period, 48 percent were documents.[1] In a year-over-year comparison, 59 percent of all malicious files detected in the first quarter (Q1) 2019 were documents, compared to 41 percent in Q1 2018—a worrisome indicator of the trend's momentum.[2]

A document is essentially an official record of information. The term covers anything from a hand-written shopping list to a printed birth certificate to a financial statement created with a computer application. Documents have become one of the most common means of spreading malware, an independent security technology analyst has noted, and embedded script can download and install other malware from the Internet.[3] Popular productivity tools such as Microsoft Word and Adobe Acrobat have become more feature rich, offering advanced macro and scripting capabilities that allow them to run processes and install bits of code on user systems.[4]

In the real world, documents typically are stored in files, tucked into folders and organized in cabinets or boxes. Similarly, a computer file is a basic data storage unit. It may consist of one or more documents, but it can include other types of data as well, such as images, music, videos, computer programs and so on.

MICK BRADY

Is a freelance technology communicator with more than 20 years of experience editing and writing for technology-focused publications.

Through extensive analysis of more than a million files, the team at Israel-based network security provider odix[5] detected something suspicious or malicious in 0.2 to 0.5 percent of email attachments submitted to its customers by their clients.

In its analysis, odix was able to break down results by file type and a variety of other characteristics. For example, the odix algorithm flagged as suspicious any file that had a binary structure inconsistent with its declared file type (e.g., a file labeled Portable Document Format [PDF] that did not have a PDF structure). In such a case, embedded malicious code could be responsible for misrepresenting the file as a PDF.

At first glance, 0.2 to 0.5 percent of potentially problematic email attachments might not seem like a serious threat, but when those small percentages are applied to large numbers, the risk becomes apparent. For enterprises that rely on document exchanges to carry out their routine operations, such as supply chain automation (SCA) platform Centersource Technologies, which helps organizations manage their shipments globally,[6] the threat level is serious and demands a response.

"We are a supply chain platform focused on the forestry industry primarily," said Amir Rashad, chief executive officer (CEO) at Centersource Technologies, which is headquartered in Sweden. "A large shipment can have up to 400 documents. It is very easy to sneak in a malicious file, which can have disastrous consequences. For a factory, producer or industrial customer that has tens of millions of US dollars in revenue—maybe even more—it would be catastrophic if all their business data were leaked or at risk."

Enterprises at Risk

Cyberthreats can impact business continuity and productivity in a myriad of ways (**figure 1**). Enterprises that have experienced cyberattacks are more likely to lose intellectual property, experience client data breaches and incur damage to their brand reputation.

Malware in documents can be especially pernicious. "In some cases, the malware uses embedded scripting to silently download and install other malware from sites on the Internet," said Rapoza. "Often these downloaded payloads take the form of the worst kinds of malware out there—rootkits that steal information from systems or botnets that make systems part of the malicious networks used to attack both organizations and networks to continue the spread of malware and spam."[7]

Other types of embedded malware mischief include stealing personally identifiable information (PII), blocking data access and launching ransomware attacks.

The Value of Being Proactive

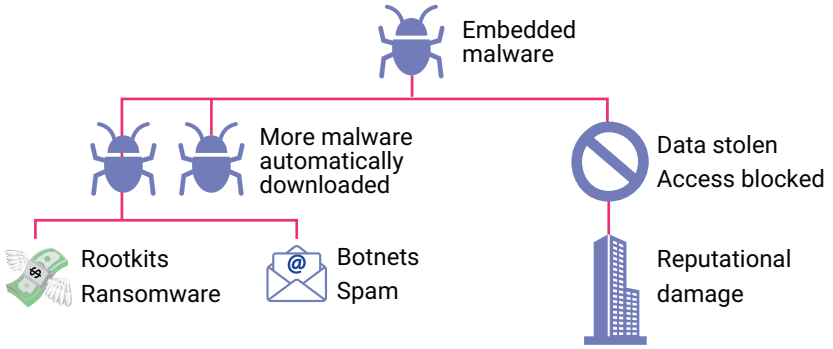
Vendors have been fighting the good fight to patch holes exploited by malware writers, but as is the case with cybersecurity in general, the black hats are often several steps ahead. The threat is not limited to spam or phishing attempts. Malware can find its way into file attachments transferred in the normal course of conducting business between parties that know each other and need the documents exchanged for legitimate purposes.

> CDR and deep file inspection constitute a highly granular, preventive detectionless approach.

Founded in 2017, Centersource has experienced rapid growth. Its Software-as-a-Service (SaaS) supply chain automation product helps move a high volume of forestry products. "Our combined user base on the platform produces, purchases or transports the equivalent of 440,000 containers every year," Rashad said.

Vendors, users and customers upload and send orders, invoices and bills of lading in Microsoft Office and PDF formats through file transfer portals at every stage of shipment, and each of those documents poses a security risk. Initially, Centersource relied heavily on detection-based malware solutions available in the market to safeguard its operations. Its security strategy did not include a file-scanning system.

FIGURE 1
Embedded Malware Risk



The young company decided not to wait until a security incident forced its hand. "Nothing had happened [in terms of a security incident], but as we grew we wanted to be proactive," said Rashad. As a platform that facilitated cooperation and data sharing among supply chain counterparts, Centersource's aim was to demonstrate an ability that surpassed the status quo in terms of minimizing malware infection risk.

In addition to drastically reducing risk, Centersource wanted a solution that would be cost-effective and easy to implement. Early in 2020, Rashad, along with the company's head of cybersecurity and its senior software developer, sought the most advanced malware prevention solutions on the market. "We looked around the market and spoke to nearly all the market leaders," Rashad recalled. The team decided to add deep file inspection technology based on content disarm and reconstruction (CDR) algorithms as an advanced security layer.

How CDR Works

Detection-based solutions, such as legacy antiviruses and sandboxes, inspect file content and behavior to determine if a file is malicious. On the other hand, CDR and deep file inspection constitute a highly granular, preventive detectionless approach.

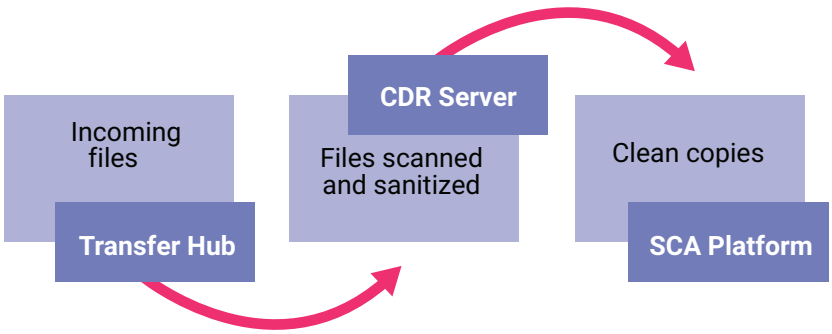
Instead of searching for known malicious code, NetFolder,[8] a solution from odix, applies an algorithm to scan files at the binary level. The technology sanitizes files by disassembling the code, removing pieces of embedded code that do not belong and then reconstructing the files. The result is that harmful code is extracted and attachments become safe to use. Everything else—the intended content,

functionality and properties—remains intact. It is not necessary to understand the nature of the problem code—all that is needed is to recognize that it is not relevant to the document.

"CDR is the most suitable technology, or maybe the only one, that really can protect you from threats in documents," said Rashad. "You might have an antivirus tool from Norton or McAfee, but that does not actually read the file on a code basis. If there is a custom-made threat against an organization, its antivirus software could pass it as green, even though there is a threat inside. As I understand it, CDR is the only solution that can catch it."

Centersource has an on-premises solution with odix's NetFolder installed on a separate server. When a user (e.g., one of its sawmill customers) uploads a file to Centersource's transfer hub, the file is sent directly to that dedicated server, where it is quarantined from the rest of the network. There it is scanned, and sanitized copies are then sent back to the system for normal handling (**figure 2**). The systems are bridged through software integration.

FIGURE 2
CDR Process



Although the CDR approach is regarded as novel in some areas,[9] it is already well accepted in certain parts of the world, notably in odix's home country, Israel.

"If you look at the players in the market, almost all of them are Israel-based organizations, because this technology was actually initiated by the Israeli Army," observed Revital Libfrand, chief marketing officer (CMO) at odix.

Most of the enterprises in the Israeli market have adopted CDR technology, Libfrand said, noting that it makes sense because almost all employees have served in the Israeli military. Military service is compulsory for Israel citizens (with some exceptions).[10] Odix CEO Oren Eytan, Ph.D., served in the Israeli army as commander of the cyber unit.

> The technology sanitizes files by disassembling the code, removing pieces of embedded code that do not belong and then reconstructing the files.

Outside of Israel, interest in CDR is growing, particularly in Europe and the United States. Analysts started to talk about it a few years back, Libfrand noted, saying that it was good to have it as an additional layer on top of the sandbox and could replace it in some scenarios.[11]

US-based OPSWAT, which odix views as the main competitor for its on-premises solution, recently raised US$125 million dollars. OPSWAT plans to use the new capital to accelerate growth, focusing on global expansion of its sales, marketing, customer success and business operations. It also plans to use the funds for further investment in research and development (R&D) innovation and to pursue strategic acquisitions.[12]

"So you do see the interest from the investment perspective," Libfrand said. "There is more interest and more traction with this technology. It took some time, but I guess enterprises do understand that using tools that are detection-based is not that efficient."

Installation and Integration

In March 2020, Centersource began evaluating the CDR technology with Eytan's assistance. During the demo process, odix illustrated the software's malware prevention capabilities in their simplest form. Files sanitized by NetFolder provided a fully functioning and malware-free format to Centersource within a few seconds, without impacting data accessibility or system latency.

Centersource decided to utilize NetFolder shortly after the first demo, according to Rashad. "It was a very simple process to implement," he said.

Centersource opted for odix's on-premises solution, providing its own private cloud hosting. The odix team supplied a folder and a product key, and Centersource set up a new server and installed NetFolder.

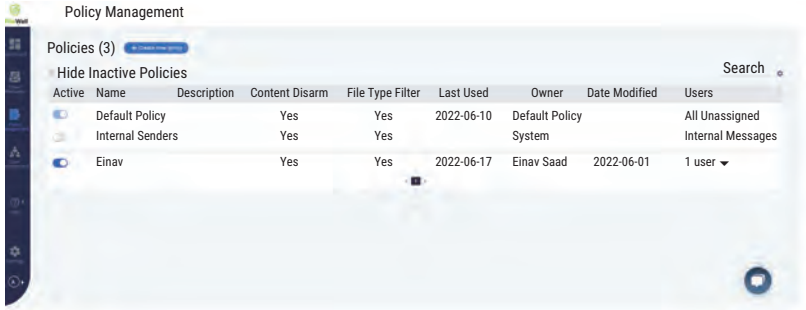
Imagine that each server is a house, Rashad suggested. "You are furnishing it and making it nice, and you make sure that the water runs and the heating works." It is separate housing, though, he continued, "because if there is an infected file that takes over the server, it should not affect the main house where everybody lives—it just impacts the summer house or the guest house."

Controlling human interactions with data is at the heart of many security strategies.

Odix trained Centersource's senior developer on the capabilities of the product and in advanced system configuration techniques, including policy definition (e.g., how to define the way active content within the file will be blocked), said Libfrand (**figure 3**).

The next step for Centersource was to integrate NetFolder with its SaaS product. "You actually need to link the two houses together so that they speak—like a bridge essentially—and that took some more time," said Rashad.

FIGURE 3
NetFolder Policy Configuration



Source: odix © 2021. Reprinted with permission.

Odix staff were on hand to supply specific answers to any questions that arose during the integration, he recalled. "For example, 'There is a package block in the bridge that will not pass. How do we make it pass?' or 'We have a false response. How can we enforce the policy that no executable files will have access to the network?'"

Those types of questions amounted only to minor hitches, however. The installation and onboarding were accomplished in a week. Now that the system is live, user files are uploaded directly to odix, and after successful scanning, downloaded to the Centersource network.

Data Exposure

Controlling human interactions with data is at the heart of many security strategies. Who handles the data, under what circumstances and for how long? These are questions likely to come up during the consideration of the use of any new information security technology. During the CDR file-scanning process, who could possibly access the data and what controls are in place?

In the case of the odix NetFolder solution, "It depends on if the deployment is cloud-based or on-premise," said Libfrand. "If it is an on-premise data center at the organization, nobody has access besides the organization." The software scans a file and then returns a sanitized copy to the application or the user.

The NetFolder software tracks the files scanned, and a management application lets the customer

LOOKING FOR MORE?

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

The CDR solution has allowed Centersource to increase the quantity and consistency of file uploads without the concern of additional exposure of its secure internal operational network to malware.

see sanitization performance, such as sanitized or blocked files.

The NetFolder management console view is available to Centersource, Rashad noted, "…but the actual sawmill company cannot see that administrator panel. The sawmill can only see its own files or those that its supply chain partners have shared with it. What it can see is that a file was uploaded, and it passed, or it did not pass."

It is a little different for the odix cloud-based product. "FileWall is a pure SaaS service providing CDR, or deep-file inspection, to Microsoft 365 email attachments," noted Libfrand. "Theoretically, nobody has access to it unless you are the administrator of the system" (**figure 4**).

The file is processed in the cloud, on the odix FileWall servers in Amazon Web Services (AWS). "We do not keep the files. We do not keep data—we are just processing," Libfrand said. "The processing is completed in a matter of seconds and then the file is no longer in our system."

Risk Reduction and Business Continuity

The CDR solution has allowed Centersource to increase the quantity and consistency of file uploads without the concern of additional exposure of its secure internal operational network to malware.

"In theory, we can handle an endless amount, but the important part is not how many more files we are managing," said Rashad. "It is that there is no concern or risk for us and our users. As a business owner, I can sleep well—not worrying about a Trojan horse at night—and in business meetings, I have an easy sales argument."

Many industrial organizations have weak or nonexistent document security, Rashad pointed out. "The forestry industry is very, very traditional. It is the old guard."

Hewing to tradition when it comes to information security can be an expensive misstep. A breach could have very negative consequences. Supply chain attacks are on the rise, and so are the costs associated with them. The average cost of a supply chain attack against an enterprise was US$1.4 million in 2021, making it the most expensive type of cyberattack.[13]

FIGURE 4

FileWall Dashboard View

Source: odix © 2021. Reprinted with permission.

"CDR is showing customers that we are very proactive despite being a young company. We take their security seriously. There is a new wave on the way in, and we are part of that wave," said Rashad. Apart from the protection against malware, the solution offers a more reliable file transfer mechanism, he noted. China has a firewall, for example, and documents critical for moving shipments through the supply chain might get blocked.

In terms of business continuity, there is less risk when sending documents to a central hub, where the recipient is notified that the documents have been shared, than there is when sending hundreds of megabytes of attachments in a single email to a single enterprise. "Because then it might be blocked and the recipient might not notice," Rashad explained. "If they do not receive the attachment and the shipment arrives—20 containers, for example—they could pretty quickly accrue hundreds of thousands of dollars in port storage and demurrage fees."

While CDR technology does not eliminate all cybersecurity risk, it does provide a valuable layer of security for enterprises that depend on the exchange of vast quantities of documents to conduct their routine business.

"Centersource users have to upload many types of official documents, so there is always a risk of hacking from infected files. After adding NetFolder, we do not have to worry about infected files anymore," Rashad said.

"Centersource's cyberrisk profile has been dramatically decreased through the use of odix's advanced deep file inspection solutions," said Eytan. "Centersource has the assurance that files shared and uploaded to its network remain secured, malware-free and fully accessible to all relevant parties."

The 0.2 to 0.5 percent of malicious files referenced previously that odix found in its analysis is concerning for any enterprise handling a large volume of documents. Because odix conducted its study using files aggregated from many sources, that result does not reflect the status or experience of any one specific organization. However, with the CDR solution now in place, the percentage of malicious files entering the Centersource system is 0.00 percent.

CDR offered Centersource an alternative to hunting down the bad actors through antivirus systems and other conventional detection-based approaches. When files go through the deconstruction process, any code that does not belong—regardless of its purpose or functionality—is omitted from the reconstructed copies. CDR disarms the enemy before it gets a chance to launch an attack, helping protect Centersource from potential financial or reputational harm.

Endnotes

1 Tanner, J.; "Threat Spotlight: Document-Based Malware," Barracuda, 4 April 2019, *https://blog.barracuda.com/2019/04/04/threat-spotlight-document-based-malware/*
2 *Ibid*.
3 *Ibid*.
4 Rapoza, J.; "The Rise of Document-Based Malware," Sophos, *https://www.sophos.com/en-us/security-news-trends/security-trends/the-rise-of-document-based-malware.aspx*
5 odix, *https://www.odi-x.com*
6 Centersource, *https://www.centersource.io*
7 *Ibid*.
8 odix, "NetFolder—Your Ransomware Protector," *https://www.odi-x.com/odix-netfolder*
9 Kolodgy, C.; "Four Startups Driving Cybersecurity Innovation," *Security Boulevard*, 23 June 2021, *https://securityboulevard.com/2021/06/4-startups-driving-cybersecurity-innovation/*
10 Jewish Virtual Library, "Israel Defense Forces: History and Overview," *https://www.jewishvirtuallibrary.org/history-and-overview-of-the-israel-defense-forces*
11 Cobb, M.; "Using Content Disarm and Reconstruction for Malware Protection," *TechTarget*, February 2021, *https://www.techtarget.com/searchsecurity/tip/Using-content-disarm-and-reconstruction-for-malware-protection*
12 Lewis, K.; "OPSWAT Receives $125 Million Investment From Brighton Park Capital to Accelerate Growth Momentum," OPSWAT, 31 March 2021, *https://www.opswat.com/blog/opswat-brighton-park-capital-investment*
13 Fadilpašić, S.; "Supply Chain Attacks Are Now More Costly Than Ever," ITProPortal, 8 October 2021, *https://www.itproportal.com/news/supply-chain-attacks-are-now-more-costly-than-ever/*