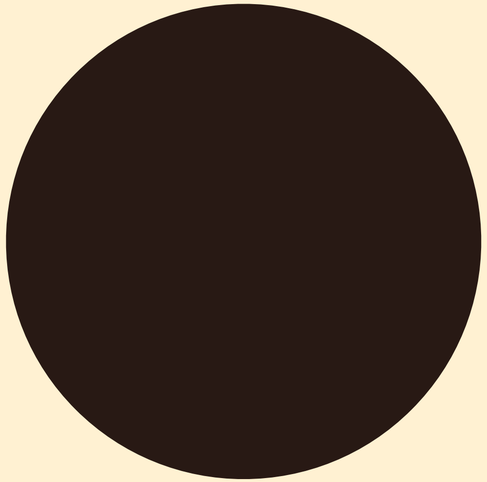
Whitepaper

DeepGuard

Proactive on-host protection against new and emerging threats

4th edition



WITH SECURE

Contents

Document history
4th Edition: October 2020
3rd Edition: October 2018
2nd Edition: June 2016
1st edition: July 2013

DeepGuard

This whitepaper explains the trends and developments in computing that have made host-based behavioral analysis and exploit interception necessary elements of computer security. It also provides an overview of the technology and methodology used by DeepGuard, the Host-based Intrusion Prevention System (HIPS) of WithSecure's security products.

DeepGuard offers dynamic proactive behavioral analysis technology that efficiently identifies and intercepts harmful behavior. When used in tandem with other components of a multi-layered security approach, DeepGuard provides light-weight and comprehensive endpoint protection with minimal impact to the user experience.

Key Features

- Updateable scanning engine uses the latest detections to protect against emerging threats.
- Continued application monitoring protects against delayed malicious actions.
- Exploit interception module recognizes and blocks exploit attempts, including document-based attacks.
- Ransomware protection module recognizes and blocks attempts to make harmful modifcations to protected files.

Benefits

- Provides immediate on-host protection against known and zero-day threats.
- Intercepts exploit attacks against programs installed on the machine.
- Intercepts attempts to encrypt files stored in protected folders.
- Recognizes and blocks suspicious activity.
- Reduces potential loss of sensitive data or privacy due to malware infection

Availability

- DeepGuard is an integral component of various WithSecure™ security products, including SAFE, Client Security, Internet Security and Protection Service for Business (PSB).
- In these products, DeepGuard is activated with default settings, but can be turned off separately.

Disclaimers

- The purpose of this document is to help customers better understand how WithSecure™ products function, and the benefits WithSecure™ DeepGuard provides. This document is not designed to be a legally binding agreement that defines the content of products and services provided by WithSecure™ Corporation.
- WithSecure™ DeepGuard, as with any of our other products and services, is a constantly evolving set of software, systems and processes. This document may become partly inaccurate as this evolution takes place. WithSecure™ Corporation will update this document every time major changes are made to our products,systems or processes. The latest version will always be available on WithSecure's website.
- Any metrics or diagrams presented in this document are valid at the time of publication. Metrics or diagrams may change over time. Presented metrics should therefore be interpreted as approximate figures.

Security challenges in a digital world

In today's world, almost all businesses and consumers have become highly dependent on speedy, reliable access to Internet-based services for their operational, recreational or personal needs. While this global movement to a more digitized world has brought tremendous benefits to organizations and individual users, one of its unintended side effects is that today, the creators and distributors of malicious software (malware) can spread their harmful products to a far wider audience, over a larger number of channels or vectors, than has ever been possible before.

In such a globalized and digitized world, security software is faced with a number of challenges:

High volumes of malware

Malware once required a certain level of technical skill to create. This is no longer the case, as builder toolkits now give even unskilled users the ability to create malware. These toolkits grew out of the 'malware-as-a-service' criminal underground, and have fueled an explosion in malware. Today, hundreds of thousands of new malware are churned out every month, in addition to millions of pre-existing malware. This overwhelming volume makes it impractical to use traditional file signatures to identify each individual threat.

Challenge: Identify and block new and existing malware, without compromising performance.

High volumes of clean programs

Harmless or clean programs number in the millions, and today are globally available online. Ideally, security software should be able to differentiate clean programs (including any updates or components) from malware, without needing to scan each one. The sheer variety and abundance of clean programs from around the world however makes it impractical to use a local whitelist or blacklist to do so.

Challenge: Identify clean files without needing to scan them, to improve performance.

Exploit-based attacks on popular programs can impact a large number of users

Some attacks use special code known as exploits to target vulnerabilities or flaws in a program that make it possible for attackers to install malware, steal data and perform other harmful actions. These attacks are a particular danger for popular programs that typically have millions of users globally, as successful exploitation can give attackers access to a huge audience of users. While software vendors usually patch any flaws reported in their products, the time needed to develop an deploy the patch still leaves a period - known as th zero-day - in which an affected program may be open to attack.

Challenge: Identify and block exploits of known and zero-day vulnerabilities in programs.

Email-based attacks constantly change to evade detection

Email remains a popular channel for attackers and malware distributors to reach their targets. To evade detection, attackers frequently alter the tactics and malware they use, making it vital that security software stay abreast with the latest intelligence on such attacks to be effective.

Challenge: Identify and block the latest malware and attacks delivered via email.

Harmful programs display a diverse range of behaviors

Different types of harmful programs have different, characteristic behavior patterns. For example, the two most high-profile types of malware in recent years are ransomware[1] and cryptominers[2]: the former steals control of a device or data and holds it for ransom, while the latter uses a device's resources to generate units of a digital cryptocurrency for the malware author's benefit.

Security software must be able to correctly identify programs that perform any of a diverse range of harmful actions, without falsely identifying clean programs that may perform similar but harmless actions.

Challenge: Identify and block programs that attempt to perform harmful actions, without impacting clean programs performing legitimate actions.

'File-less' attacks hide by forcing other programs to act for them

'File-less' attacks do not install their own executable files; Instead, they exploit or abuse installed programs or components of the operating system and force them to perform harmful actions.

Challenge: Identify and block harmful actions by programs that have been exploited by malware.

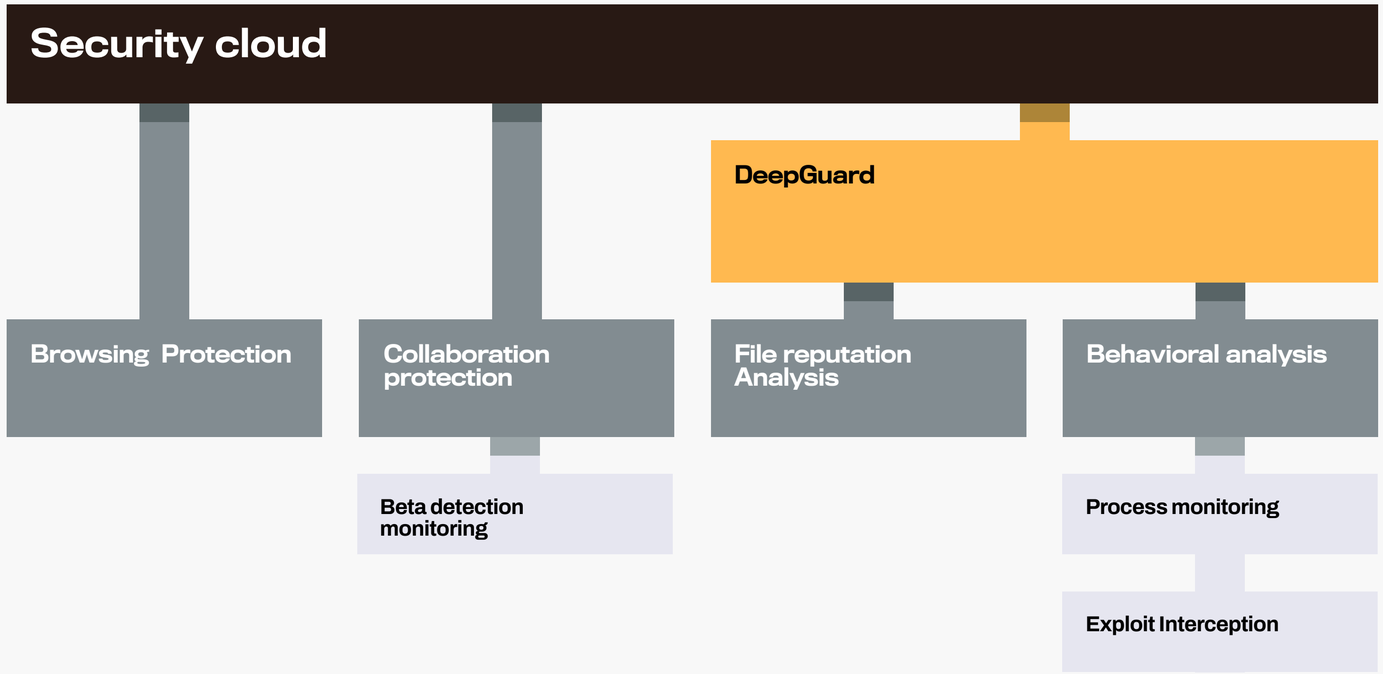
To protect users, their devices and data in such a demanding environment, WithSecure's proactive endpoint security software use a multi-layered approach that includes: website security verification, file scanning, cloud-based file and web reputation checking, behavioral analysis and a Host-based Intrusion Prevention System (HIPS).

Multi-layered protection

WithSecure's multi-layered approach to security is comprised of the following modules, each designed to address a particular security challenge, and all intended to work together to provide a complete solution: of websites online, Browsing protection can also connect to a database of known safe and harmful sites in WithSecure's Security Cloud, a cloud-based network hosting specialized databases and automated analysis systems.

Browsing protection

Today, users are most likely to be exposed to attacks or malware when they are online. This means that the earliest stage of protection begins by preventing the initial exposure to possible sources of attack or malware. Enter Browsing protection, which provides users with a critical assessment of a website’s security. If a site is known to be harmful, or has features that render it suspect, Browsing protection displays a clear cautionary message to the user, so they can avoid visiting the site. To keep up with the latest intelligence on the millions of websites online, Browsing Protection can also connect to a database of known safe and harmful sites in WithSecure's Security Cloud, a cloud- based network hosting specialized databases and automated analysis systems.



File scanning engines

If a suspect file does still make it onto a computer or device - whether downloaded from an unrated site, or delivered via another channel, such as removable media - it is scrutinized by the next layer of security checks. When the file is first installed or modified, file scanning engines scan it using algorithms or detections which identify code or behavior that match known malware. While hardly new technology, code-based detections such as this still effectively detect the vast majority of older threats that are still circulating today. Separately, a beta detection monitoring module notifies the Security Cloud if any experimental detections would have been triggered by the suspect file's code or actions. This gives crucial feedback to WithSecure's Labs on the detections' effectiveness, so that analysts can fine-tune their logic to avoid false positives.

DeepGuard

If the file scanning engines are unable identify a suspect file as either clean or a known threat, more sophisticated technology is brought into play. The suspect file now comes under the scrutiny of the DeepGuard module, which first checks with the Security Cloud if there have been any previous reports about the file to indicate if it is safe or harmful. If there is no prior record, the module then begins monitoring the file's behavior, at both the point of launch and while it is running. If at either point the file performs actions that appear to be harmful, or shows any characteristics of an exploit attempt, it is immediately blocked from continuing.

Security Cloud

While on-host solutions provide immediate local analysis, many users express concerns about the storage and performance impact that security products can have on their machines. To address these concerns, if an Internet connection is available and an administrator permits it, WithSecure™ security products can communicate with the Security Cloud, where they can perform more intensive analysis on new files or retrieve the latest details of threats already seen in the wild by other clients, making response far more efficient and effective.

In addition, WithSecure™ Labs analysts actively monitor the threat landscape for new threats and research the most effective ways to detect malware, which go into updates to the rules used by the databases and analysis systems. The updates then take 60 seconds to replicate across all products connected to the Security Cloud, ensuring that they always have the latest threat intelligence.

More about security cloud

- Reputation queries are performed over secure HTTPS connection to our Karma-service
- Queries are anonymized and the IP address is not stored, to maintain the client's privacy
- The network's infrastructure is hosted on servers in multiple data centers around the world
- The automated analysis systems make up to 8 million risk assessments per day

For more information, see:

- WithSecure™ Security Cloud: Purpose, function and benefits (PDF)
- WithSecure™ Security Cloud privacy policy

Introducing DeepGuard

The DeepGuard module in WithSecure's security products is a Host-based Intrusion Prevention System (HIPS), which performs file reputation analysis and behavioral analysis. This module is responsible for the proactive, on-the-fly monitoring and interception that serves as the final and most critical line of defense against new threats, even those targeting previously unknown vulnerabilities.

File reputation analysis

Before DeepGuard starts the more intensive behavioral analysis, it first checks a suspect file's reputation in the Security Cloud - that is, any existing information or security assessment about the file that shows whether it can be trusted.

Reputation query

During this check, DeepGuard sends a query to the Security Cloud to retrieve the latest information on a suspect file's reputation. If it has already been seen and reported by another client, the file will have an existing evaluation that DeepGuard can immediately use to decide if it can be trusted. If it is new, anonymized metadata about it (e.g, file size and path) is sent to the Cloud's automated analysis systems, which evaluates the metadata together with information drawn from in-house databases and other sources and returns a comprehensive, up-to-date risk assessment for the file. This reputation check greatly improves the security product's performance, as it avoids unnecessary scans on known files.

Prevalence rate check

DeepGuard also uses prevalence rate checks to determine if a file is trustworthy. This check depends on the fact that clean programs are used by a large percentage of our customer base - that is, they are highly prevalent. These programs also change infrequently, making them easy to whitelist and track in a database of clean files. In contrast, malware are comparatively rare - that is, they have low prevalence. This check filters out known clean files so that DeepGuard can concentrate on new or unknown ones, improving both performance and accuracy.

Behavioral analysis

Before DeepGuard starts the more intensive behavioral analysis, it first checks a suspect file's reputation in the Security Cloud - that is, any existing information or security assessment about the file that shows whether it can be trusted.

DeepGuard's behavioral analysis is split into three focus areas to address specific challenges:

Process monitoring

While a program runs, DeepGuard monitors its behavior for any actions that might cause harm to the system or to data stored on it.

Exploit interception

DeepGuard monitors programs known to be targeted by attackers, and blocks any actions that bear the hallmarks of a vulnerability exploit. It also looks for and blocks document files that contain exploit code.

Ransomware protection

DeepGuard looks for and blocks any programs that try to modify files stored in specially-designated 'protected folders'.

Cloud-based analysis modes

In addition to on-host behavioral analysis, the Security Cloud also provides two cloud-based analysis modes.

First is metadata-based analysis where Security Cloud provides intensive processing power to run various tools to extract features from a suspect file. The metadata collected from the tools will be aggregated with the metadata sent from the endpoint client to provide more context on the attack which enables more in-depth analysis.

Second is a cloud-based dedicated sandbox solution that can thoroughly inspect suspect files either in a selfcontained, virtual environment without affecting the local system's performance. The verdict from this cloudbased system is made available to DeepGuard. This inthe- cloud metadata-based and behavioral analysis are especially useful for the kind of in-depth inspection needed to identify unique malware that have been specially-crafted to fit the victim; as such highly tailored threats typically have no known signatures, metadata-based and intensive behavioral analysis are the most effective ways of stopping them.

How DeepGuard works

DeepGuard is activated by two events: when a program is launched for the first time, and while a program is running (that is, during its runtime). During each event, DeepGuard performs either file reputation analysis or behavioral analysis.

At launch

When a program is first launched, regardless of how it is done (the user clicks the file icon, an email attachment or program initiates it, etc.), DeepGuard temporarily delays it from executing and performs the following checks:

File reputation check

DeepGuard sends a query to the Security Cloud to retrieve the suspect file's reputation details. The query is sent using the strongly encrypted Object Reputation Service Protocol (ORSP), is completely anonymized and the IP address is not stored, to maintain the client's privacy.

If the file has been previously seen and reported by other products connected to the Security Cloud, the automated analysis systems will have performed and saved a security assessment of it that indicates if the file should be considered trustworthy or harmful. If DeepGuard's query to the Security Cloud about the file it is analysing returns the verdict that it is a threat, DeepGuard immediately blocks it from launching.

Prevelance rate check

DeepGuard also queries the Security Cloud for the file's prevalence rate.

Rare or new files are automatically considered more suspect and subjected to greater scrutiny during the subsequent process monitoring stage.

Judgement on execution

At this stage, based on the file's reputation, DeepGuard makes one of the following choices:

1. The file is clean and allowed to execute normally
2. The file is harmful and blocked from executing
3. The file's status as clean or harmful is still unknown

If the file is blocked from launching, a notification message is displayed providing additional details and an option to whitelist the program, if desired.

If the status of the file is still unknown, DeepGuard allows the file to execute but continues to monitor it during the subsequent process monitoring stage.

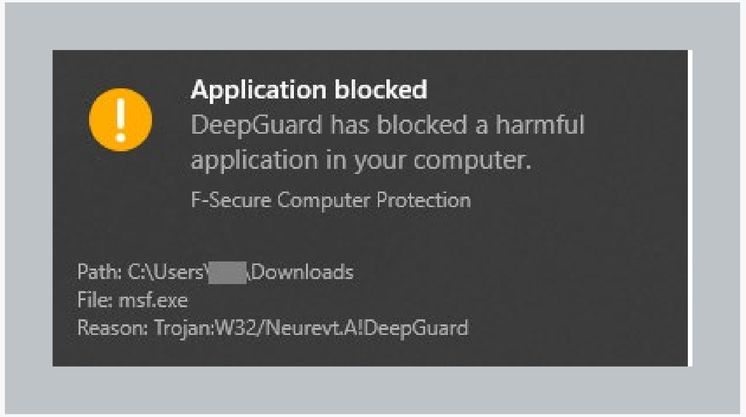


Image 1. DeepGuard displays a notification message after blocking a harmful application from running

During runtime

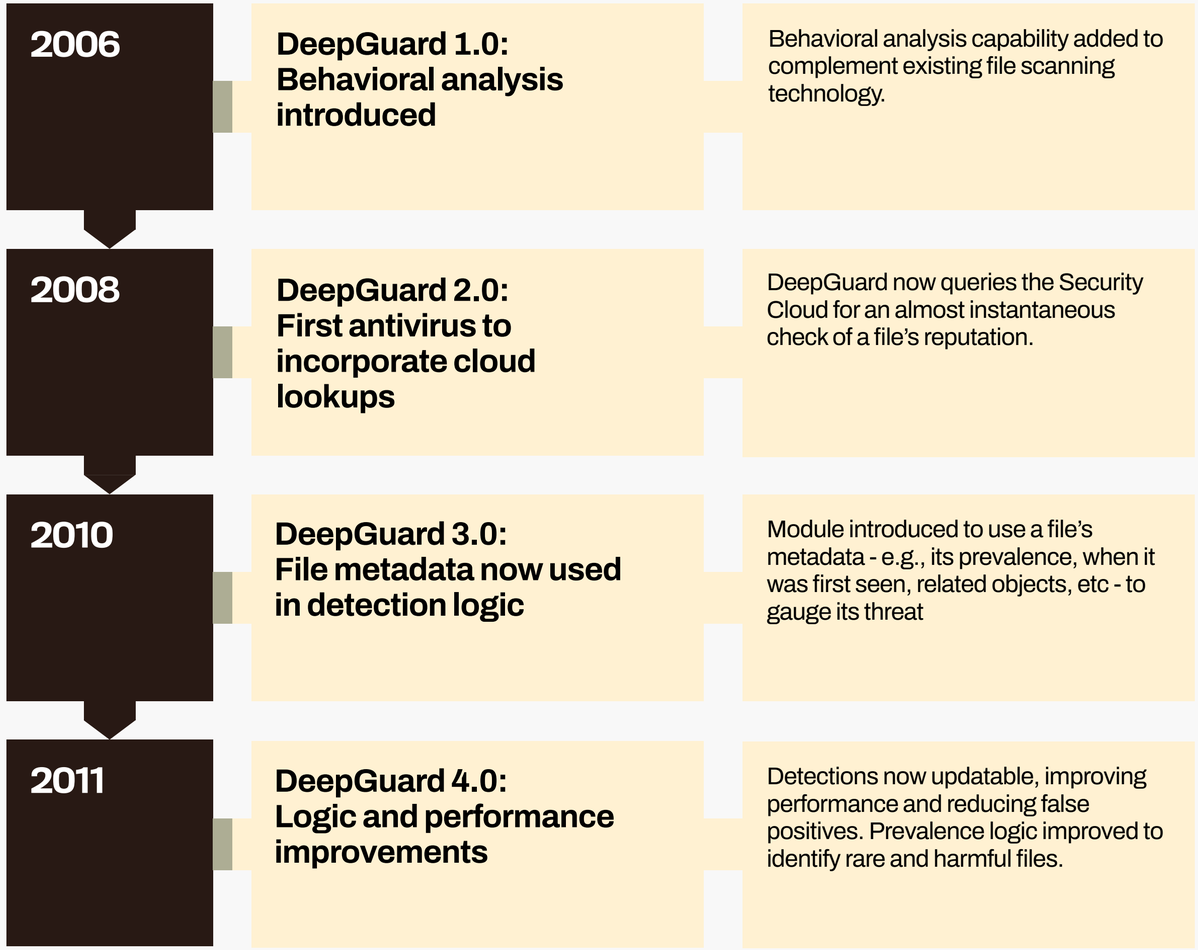
If a program passes the file reputation analysis and is executed, DeepGuard begins to monitor its behavior as a precaution against delayed harmful routines, a common tactic used by malware to circumvent pre-launch checks. This quiet vigilance allows DeepGuard to provide constant protection without disrupting the user's experience with constant prompts.

Process monitoring

A program's processes are blocked from continuing if DeepGuard sees it performing a number of suspicious actions, which may include (but are not limited to):

- Modifying the Windows registry
- Editing files in certain critical system directories
- Injecting code in another process's space
- Attempting to hide processes or replicate themselves

As clean programs will also perform such actions from time to time, a critical threshold of multiple suspicious actions must be reached before DeepGuard will block the process. If available, file reputation and prevalence rating information from the Security Cloud is taken into account to determine this threshold. For example, DeepGuard treats a file with low prevalence more aggressively by lowering the threshold of actions it can perform before the file is blocked.



Exploit interception

DeepGuard intercepts attempts to exploit vulnerabilities (including zero-days) in installed programs by monitoring the behavior of programs that are commonly targeted for exploitation, as well as those that run document files that are commonly used to deliver exploits.

Monitoring exploit-prone programs

Highly popular programs (e.g., web browsers, the Microsoft Office or Adobe business suites and video players) are far more likely to be targeted by attackers and malware for vulnerability exploitation. Because they are more likely to be exploited, DeepGuard keeps these programs under especially close watch and if they appear to be performing harmful actions, are blocked more aggressively.

Not surprisingly, given how rapidly a program's popularity can change in today's world, the list of programs that DeepGuard pays closer attention to can be updated by WithSecure™ Labs analysts when needed to stay up-to-date with the latest changes in the threat landscape.

Monitoring for document-based exploits

Document files, such as Word or Excel files, have become popular delivery vehicles for attackers. These are usually embedded with exploit code for vulnerabilities found in programs installed on a target's computer or device; the files are then attached to emails and sent to the target.

To intercept these document-based exploits, DeepGuard closely monitors any programs that open document files for suspicious behavior that could have been caused by the exploit code. By focusing on the behavior of programs that use document files, DeepGuard can pinpoint exploit attempts without needing prior knowledge of a document file, or even of the specific vulnerability being targeted, making this an effective counter against previously unseen malware that target zero-day vulnerabilities.

Ransomware detection

Ransomware will modify files on a computer or device by encrypting or scrambling them to be completely undecipherable without the correct decryption key; payment is then demanded by the ransomware's operators in return for this decryption key so that the affected files can be restored.

To counter this, WithSecure™ security products allow users to set up specially-designated 'protected folders'. Once established, DeepGuard will block any programs that try to modify files stored in these folders, and display a message notifying the user about the attempt. Users can still manually allow a program to modify the files on the notification message itself, or pre-emptively whitelist selected programs that are allowed to modify these protected files.

2013	**DeepGuard 5.0: Enhanced protection against exploit-based attacks**	Module introduced to monitor the runtime behavior of commonly targeted programs and potential attack files, allowing DeepGuard to intercept exploit-based attacks, regardless of the specific vulnerability targeted.
2016	**DeepGuard 6.0: Performance and precision improvements**	Behavioral detections further streamlined via algorithm optimizations and by utilizing modern operating system features. On-the-fly behavioral analysis is performed more accurately and with lower system impact.
2017	**DeepGuard 6.2: Ransomware protection introduced**	Module introduced to monitor and block programs attempting to modify files stored in designated 'protected folders'.

Intercepting document-based exploits

The most common delivery vehicle for exploits remains document files, which are usually crafted to appear authentic. If an unsuspecting user were to open the file, harmful code embedded in the file is run, which can result in the system being compromised.

Case in point

A suspicious email message was received with an attached Microsoft Word file named, ‘Form- 9566073483336.doc‘.

When the file was launched in the Word program, it displayed a notice prompting the user to click the ‘Enable content’ button on the security warning notification message. Doing so would allow macros, or a script of commands embedded in the file, to run.

In this case, the file contained a macro with instructions that DeepGuard recognized as harmful exploit code, with the detection Exploit:W32/CmdStager.A!DeepGuard. The application’s processes were immediately intercepted and blocked, preventing the exploit from succeeding.

Subsequent analysis found that if the exploit had been successful, it would have installed the Emotet trojan, which can steal sensitive information from the user’s computer, as well as download and install other malware.

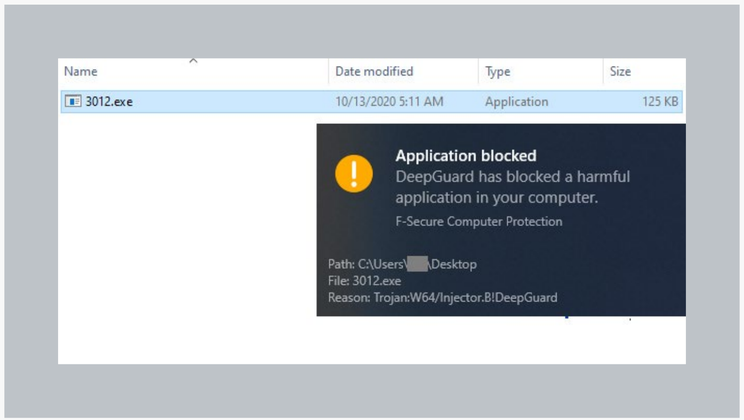


Image 2. Document file with malicious macro

Intercepting ‘file-less’ attacks

There are various methods attackers use to carry out a ‘file-less’ attack; a particularly popular way involves abusing PowerShell with a script-based approach. PowerShell is a legitimate command-line tool in the Windows operating system that can be used by system administrators to automate various tasks for managing the computer. A key feature is its ability to load and run a script directly in memory. This feature makes PowerShell a popular target for attackers, as they can abuse it to run harmful code directly in memory, rather than embedding the code in an executable file that must be saved on the disk, where it is vulnerable to detection by security products.

Case in point

The script above was received as part of a customer case and shows one method that attackers try to abuse PowerShell. This script includes the command -executionpolicy bypass, which makes a configuration change to bypass the execution policy that stops PowerShell from remotely executing commands. This would allow an external attacker to later remotely instruct PowerShell to perform further harmful actions. The script also includes a command to connect to a remote website, either to receive additional commands or to download other harmful files. Because DeepGuard is monitoring PowerShell’s actions however, its bypass of the execution policy and subsequent attempt to connect to a harmful site triggered the behavioral detection Exploit:W32/PowerShellstager.B!DeepGuard, which caused the product to immediately block any further actions and close PowerShell to prevent any further potential harm.

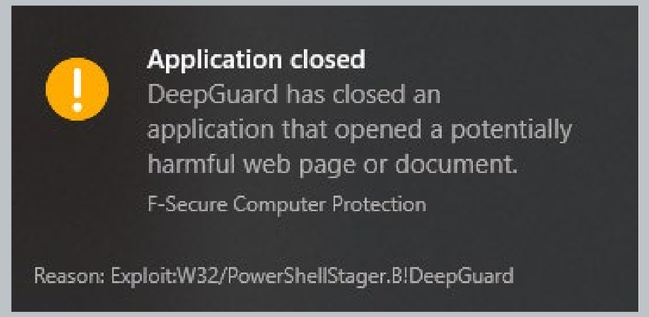
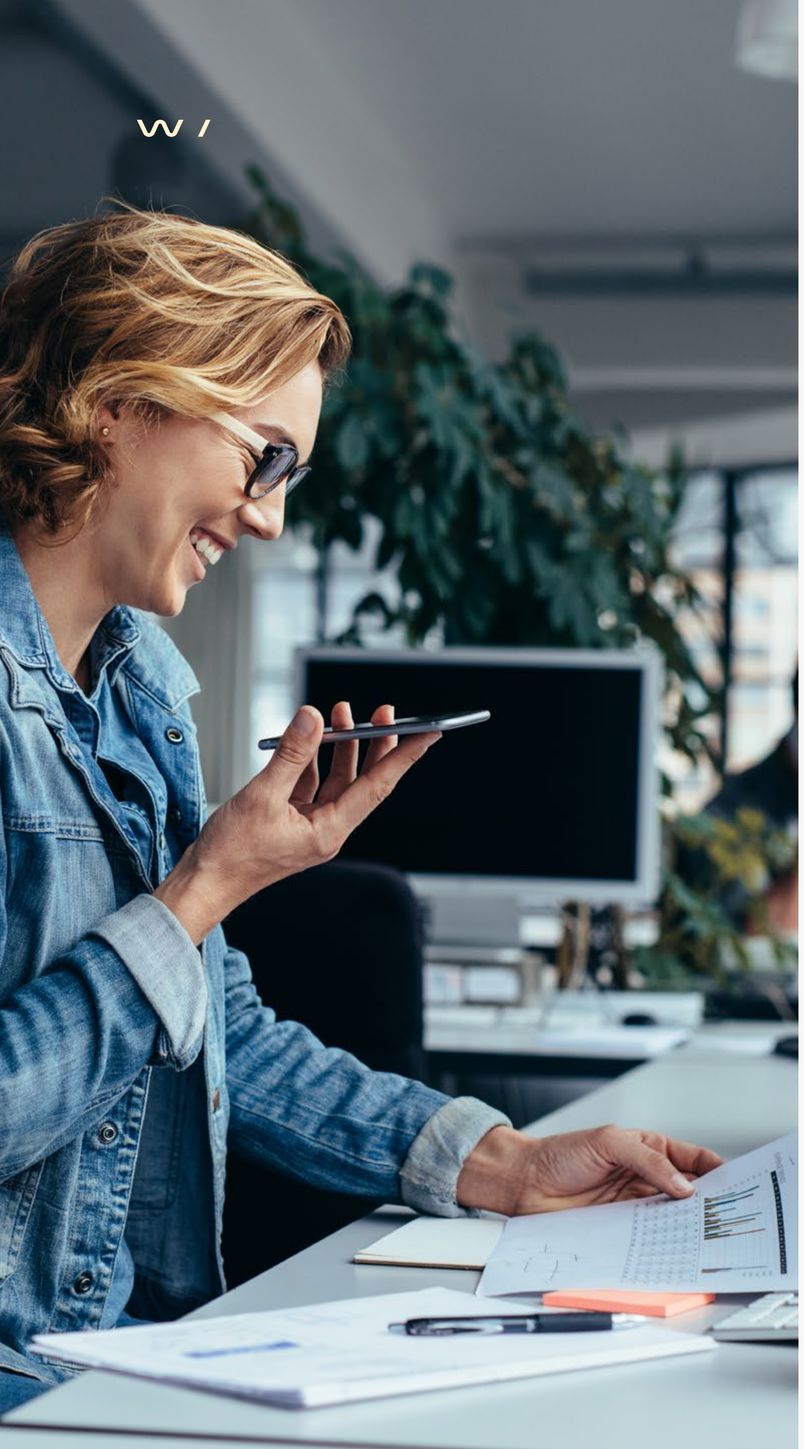


Image 3. Powershell exploit script



Detecting Crypto-ransomware

Ransomware are programs that uses alarming messages or tactics to extort money from a user. Crypto-ransomware is ransomware that encrypts or digitally ‘scrambles’ the files on a computer or device, essentially taking them hostage. A ransom payment is demanded for a decryption key that restores the affected files. Because the encryption used on the files is often extremely difficult to break, crypto-ransomware infections can be severely disruptive, especially if they infect computers in major corporations or organizations.

Case in point

In this case, a suspicious file named 3012.exe was received. As an unknown file, when it was first launched its behavior was monitored by DeepGuard; its actions subsequently triggered the detection Trojan:W32/ Injector.A!DeepGuard, which blocked the file from continuing to run.

Deeper analysis of the file showed that it would have installed and run the Ryuk crypto-ransomware, which encrypt all files stored on the affected machine, then demand a ransom payment.

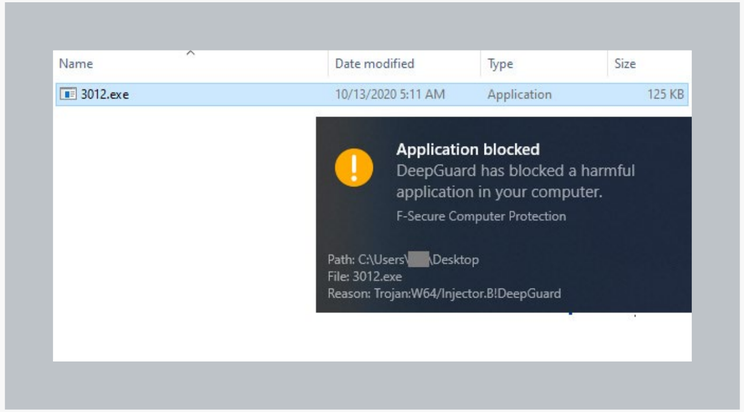


Image 4. Ryuk ransomware file

Conclusion

WithSecure's security products use a multi-layered approach comprised of multiple components that address challenges presented by threats seen in the real world. The behavioral analysis and process monitoring functions performed by DeepGuard are critical in identifying and blocking the most sophisticated malware prevalent today.

DeepGuard provides immediate, proactive on-host protection against new and emerging threats by focusing on malicious application behavior, rather than through static identification of specific known threats. This shift in focus allows DeepGuard to identify and block even previously unseen malware based on their behavior alone, neatly providing protection until security researchers can analyze and issue a detection for that specific threat.

Through lookups to WithSecure's Security Cloud, DeepGuard is also able to use the latest file reputation information available for any previously encountered object to fine-tune its security evaluations, reducing the risk of false positives or redundant analyses that can interfere with the user's experience.

DeepGuard's on-host behavioral analysis effectively intercepts attacks attempting to exploit vulnerabilities in popular programs in order to install malware onto the machine. DeepGuard can identify and block routines that are characteristic of an exploit attempt, preventing exploitation and in turn, infection. Exploit interception safeguards users from harm even when vulnerable programs are present on their machine.

DeepGuard also effectively counters the threat of ransomware hijacking control of critical data by intercepting and blocking attempts to modify files stored in specially designated folders. This on-the-fly behavioral monitoring ensures the users' data remains protected even against currently undetected or emerging threats.

In conclusion, DeepGuard combines sophisticated scanning engine technology with the technical expertise of WithSecure™ Labs analysts to perform accurate, fine-grained on-host behavior- and reputation-based analysis that ultimately significantly improves the user's security.

References

1. WithSecure™: What is ransomware?
   https://www.f-secure.com/en/home/articles/what-is-a-ransomware-attack
2. WithSecure™ Blog; Ransomware Out, Cryptojacking In?
   Latest Cybercrime Trends; published 12 July 2018;
   https://blog.f-secure.com/podcast-ransomware-cryptojacking-cybercrime/
3. WithSecure™ Labs; WithSecure™ Security Cloud: pose,
   function and benefits; published October 2015
   https://www.f-secure.com/documents/996508/1030745/security_cloud.pdf
4. WithSecure™ Security Cloud privacy policy
   https://www.f-secure.com/en/web/legal/privacy/sec

Who We Are

WithSecure™ is cyber security's reliable partner. IT service providers, MSSPs and businesses along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection & response is powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ is part of F-Secure Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

W / T H®
secure