DEEPGUARD

Proactive on-host protection against new and emerging threats

Updated: 14 June 2016

F-Secure

DEEPGUARD

SUMMARY

This whitepaper explains the trends and developments in computing that have made host-based behavioral analysis and exploit interception necessary elements of computer security and provides an overview of the technology and methodology used by **DeepGuard**, the Host-based Intrusion Prevention System (HIPS) of F-Secure's security products. DeepGuard offers dynamic proactive behavioral analysis technology that efficiently identifies and intercepts malicious behavior. When used in tandem with other components of a multi-layered security approach, DeepGuard provides lightweight 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.

Benefits

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

CONTENTS

F-Secure

THE CASE FOR PROACTIVE BEHAVIORAL ANALYSIS

One of the most demanding challenges security programs have had to address in the last few years has been the increasing diversification of attack vectors through which malware can arrive onto a host machine, especially as more applications, networks and services become hosted on or accessible over the Internet. This has been of particular concern with the growing popularity of online-based attacks that exploit vulnerabilities in applications installed on a machine in order to run malicious code.

Some of the difficulties involved in dealing with modern attacks stem from major changes in the threat landscape that have taken place in the last ten years or so, including:

Exponential growth in malware

Since the mid-2000s, when malware creation kits that automated the process of producing malicious programs first became widely available, the numbers of malware samples seen by antivirus labs have grown exponentially, with hundreds of thousands of new or variant strains being created and propagated every month. In addition to the overwhelming numbers, many of these variants are designed to live only for a short time, sometimes only days or hours, in a deliberate attempt to overwhelm antivirus programs by sheer volume.

Attacks move online

The days when malware was most commonly distributed via e-mail attachments are long gone. Today, the most common attack vector is through a silent drive-by download during a visit to a compromised legitimate site or a malicious website that hijacks traffic from search engines or compromised sites.

By moving distribution from direct delivery to the target machines to the nebulous online world, malware distributors and attackers not only increase their target audience but also make it much harder to prevent infections. Without a mechanism to identify the attack site and prevent users from visiting it, the user's machine can be successfully exploited without any overt sign that an attack has occurred.

Malware becomes a cyber crime tool

The consequences of an infection have also changed as organized criminals increasingly engage in cyber crime. Data and identity theft and monetary fraud are all criminal activities that have in recent years been facilitated by malware, in some cases in staggering amounts.

For example, the United States Federal Bureau of Investigation (FBI) reported in June 2015 that the losses incurred by victims affected by a single ransomware[1] family had totalled over USD18 million[2]. With most real-world authorities lacking the resources or political will to prosecute cyber crimes, there is strong monetary incentive for cyber criminals to continue and improve their online activities.

Popular software is heavily targeted

Although almost any software can contain vulnerabilities, of particular interest to cyber criminals and other attackers are vulnerabilities in popular applications, such as Adobe Flash Player, Microsoft Office and web browsers. These programs typically have millions of users, making them prime targets for attack. Many of these applications have multiple known vulnerabilities, and though most are fixed by security patches released from the vendors, the time needed to develop and deploy these fixes to all affected machines still leaves an interval in which the users are vulnerable.

DISCLAIMERS

- The purpose of this document is to help customers better understand how F-Secure products function, and the benefits F-Secure DeepGuard provides. This document is not designed to be a legally binding agreement that defines the content of products and services provided by F-Secure Corporation.
- F-Secure 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. F-Secure 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 F-Secure'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.

"MALWARE IS CONSTANTLY EVOLVING, WITH NEW TRICKS AND FEATURES. BUT ONE THING REMAINS CONSTANT - MALWARE WILL ALWAYS EXHIBIT MALICIOUS BEHAVIOR."

Mika Stahlberg
Chief Technology Officer,
F-Secure Security Research
& Technologies

Additionally, new or zero-day vulnerabilities are periodically found for which no patches are yet available, leaving the users wide open for exploitation.

Exploit kits make attacking easier

The advent of commercial-grade exploit kits such as Angler, Neutrino or Magnitude, which automate the process of scanning and exploiting a user's machine within seconds of a visit to an attack website, have significantly lowered the level of technical expertise needed for cyber criminals to successfully infect new victims with malware.

Exploit kits have transformed vulnerability exploitation from a niche activity into a common attack vector. They have also become one of the most popular ways for malware distributors to spread their wares. For example, in April 2016, F-Secure Labs observed the following malware - a mix of ransomware and trojans - being distributed by notable exploit kits:

PAYLOADS OF NOTABLE EXPLOIT KITS IN APRIL 2016

	EXPLOIT KITS			
	Angler	Nuclear	Magnitude	Neutrino
PAYLOADS	TeslaCrypt	Locky	Cryptowall	Cerber
	Bedep			DNA Locker
	Gootkit			
	Ursnif	TeslaCrypt	Cerber	Gootkit
	CryptXXX			CryptXXX
	Mobef			

The popularity of such exploit-based methods for spreading threats has in turn led to a need for on-host security solutions that are able to identify and block attempts to exploit vulnerabilities in installed programs.

Targeted attacks make detection harder

More focused targeted attacks can involve more obscure exploits and delivery mechanisms. These attacks typically use document or executable files carefully crafted to fit the profile of the intended victim, taking into account their topics of interest, preferred operating system and any security programs they may be using.

Identifying clean programs becomes more critical

The number of clean or non-malicious applications globally available today runs into the millions, far more than the normal user is likely to be familiar with at any one time. The abundance of programs, their easy accessibility over the Internet and the need to stay abreast of constant program updates all makes it cumbersome for security solutions to depend solely on local user-driven white- and black- listing to provide adequate protection.

The majority of programs seen on a typical machine are clean, so correctly identifying non-malicious software is a significant step towards pinpointing truly harmful programs for further attention. Eliminating false positives on clean files is also critical in optimizing a security program's performance and of course, minimizing interference with the user's experience.

Given the various challenges presented by today's more complex computing realities and more fluid threat landscape, file scanning engines are now just one layer of a multi-tiered approach to endpoint security. Cloud-based file and web reputation checking, behavioral analysis and a Host-based Intrusion Prevention System (HIPS) have all become integral components of the modern proactive protection system.

MULTI-LAYERED PROTECTION

F-Secure's multi-layered approach to security is comprised of the following modules, each designed to address a particular aspect of the threat landscape and work together to provide a complete solution:

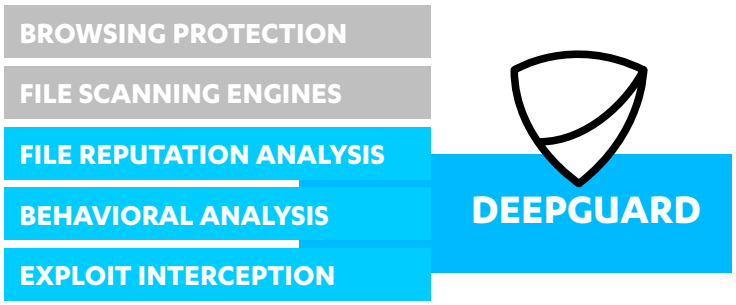
As mentioned before, most attacks and malware downloads today take place online. Ideally, protection should begin even before the machine environment is reached, by preventing exposure to possible infection points - and so, enter Browsing protection.

To prevent users from inadvertently visiting compromised legitimate or outrightly malicious sites, Browsing protection provides critical assessment of a website's security. If the site is known to be malicious, or contains features that render it suspect, the user is cautioned against entering it. To deal efficiently with the millions of sites available on the Internet and their constantly fluctuating changes in security, Browsing protection's functionality is based on lookup queries to F-Secure's Security Cloud (see page 6), which includes a database of known safe and malicious files and websites. The entries are updated automatically in real-time based on rules maintained by F-Secure Labs analysts.

Though Browsing protection is able to prevent most visits to known malicious sites, it's always possible to stumble onto an unrated or newly compromised or malicious site, or for malware to be introduced onto the host machine some other way, perhaps on removable media. If a suspect file does successfully arrive on the machine, it is then subjected to multiple layers of security checks.

Whenever a file arrives on a machine, is installed or modified, it is first scanned using a file scanning engine to determine if it is a known threat. File scanning engines use custom, family, generic and heuristic detections, which respectively identify specific malware, families of malware with similar features, and broad ranges of malicious physical features and behavior patterns. If the file's characteristics match those of previously seen malware, it is blocked.

F-SECURE'S MULTI-LAYERED APPROACH TO SECURITY



Though often overlooked in favor of more sophisticated technology, file scanning engines are still an effective method of identifying and blocking the vast majority of malware seen to date, protecting users against lingering threats such as Downadup[3] or Sality[4], which debuted and peaked years ago but are still present in the wild, where they continue to infect new victims.

If the file isn't identified as a known threat, a query is sent to F-Secure's cloud infrastructure to gather the latest metadata available for the file. Analysis is subsequently handled by DeepGuard, which collectively handles all the behavioral analysis, process monitoring and exploit interception of suspect files, both at the point of application launch and during execution.

THE ROAD TO DEEPGUARD

Heuristic analysis technology introduced

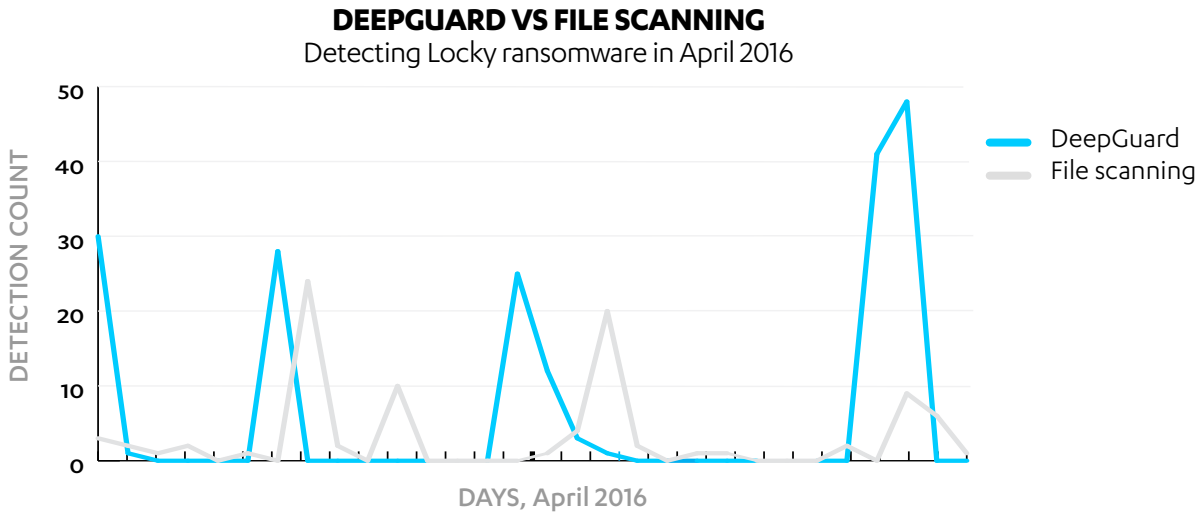
2006 DeepGuard 1.0 introduces behavioral analysis to complement existing file scanning technology. Programs that show no features or behavior matching known malware are allowed to execute as normal; those with tell-tale characteristics or malicious routines are blocked from execution

First AV product to incorporate cloud lookups

2008 In addition to file scanning, DeepGuard 2.0 queries the Security Cloud for an almost instantaneous check of a suspect file's reputation. F-Secure Labs analysts constantly monitor and update the file reputation database, providing crucial human intelligence to the automated process.

File metadata used in DeepGuard detection logic

2010 DeepGuard 3.0 includes a component that uses a file's metadata - e.g., the file's rarity, when it was first seen, related objects, and more - to gauge its threat potential. This feature allows malware to be identified using reputation-based factors such as whether the file was downloaded from a known malicious site, without needing further examination of its features or behavior



MORE ABOUT DEEPGUARD

Given the short-lived nature of most malware variants, the detections created for file scanning approaches tend to lose effectiveness rather quickly. In contrast, behavioral detections can effectively identify malware over a much longer time period, as malware behavior is much less mutable.

DeepGuard observes an application's behavior and prevents any potentially harmful action from successfully completing. The apparently simple nature of this task belies its importance however, as this proactive, on-the-fly monitoring and interception serves as the final and most critical line of defense against new threats, even those targeting previously unknown vulnerabilities.

Behavior-based analysis addresses the Achilles' heel of file scanning approaches: the need for analysts to have an actual sample of the malware in order to create the signature to identify it. Given the huge numbers of malware constantly being created and distributed, new samples must be acquired and analyzed prior to detections being created.

Behavior-based detections cover that crucial gap between the first appearance of new malware and a detection being issued for the threat. By moving the focus from structural to functional characteristics of a sample, DeepGuard can identify and block programs performing harmful actions, even before an actual sample has been acquired and examined. For example, in April 2016, DeepGuard detected and blocked files that attempted to encrypt stored files. Subsequently, signature databases were updated to flag these files (chart above) as Locky ransomware, but for users facing new threats, DeepGuard's proactive analysis provided immediate protection against infection.

In 2011, an entirely rewritten DeepGuard engine was introduced that included (among numerous other improvements) a switch from using hard-coded scanning logic to an updateable detections database. F-Secure Labs analysts constantly monitor the threat landscape and analyze the latest threats to determine the best way to identify malicious behavior. Being able to update the engine with the results of this research keeps DeepGuard consistently effective against the latest threats.

Prevalence logic increases effectiveness against rare files

2011 DeepGuard 4.0 revises the file scanning engine to use updateable detections and beta detections for false alarms reduction. It also improves the prevalence logic used to identify files that are both rare and malicious, a feature that proves decisive in winning both AV-Comparative's 2011 *Product of the Year* award and AV-Test's 2012 *Best Protection Award* [5]

Enhanced protection against exploit-based attacks

2013 Malware infections facilitated by exploits targeting vulnerabilities in common applications have become a favored attack vector. DeepGuard 5.0 introduces enhanced behavior-based detection logic, including a module that monitors the runtime behavior of commonly targeted programs and potential attack files. This broad behavioral analysis approach allows DeepGuard to identify and intercept exploit-based attacks, regardless of the specific vulnerability targeted

Performance and precision improvements

2016 With the introduction of DeepGuard 6.0, behavioral detections are 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.

Also in 2011, DeepGuard was updated to use prevalence rate checks in its detection logic [6]. This feature was a logical corollary of the fact that legitimate software are usually found installed by a large percentage of our customer base - that is, they are highly prevalent. These files also change relatively infrequently, making them easy to whitelist and track in a 'clean file' database. In contrast, files that have low prevalence quite often turn out to be malware. According to statistics generated from F-Secure's internal systems monitoring known threats, in a random sample of malicious programs found in the first four months of 2013, 99.7% of the threats were rarely seen in our user base. DeepGuard's prevalence rate check helps filter out known clean files from suspicious unknown ones, improving both performance and accuracy.

DeepGuard's updateable detection logic is especially useful in countering attacks that exploit vulnerabilities in installed programs in order to run malware on a machine. In such cases, the dropped malware itself can be spotted and blocked by file scanning engines. To halt the attack at an even earlier stage however - that is, at the point of exploitation - F-Secure Labs analysts examine the exploit mechanism for tell-tale actions or behavior patterns, and then incorporate the research results into DeepGuard's scanning engine. It is then able to pinpoint and block suspicious actions that bear the hallmarks of a vulnerability exploit attempt, preventing malware from being dropped on the machine at all.

By taking into account characteristic exploitation mechanisms as well as the features and behavior of malware being dropped on the system, DeepGuard can effectively identify and block threats on the fly, even when faced with totally new malware targeting zero-day vulnerabilities.

HOW DEEPGUARD WORKS

DeepGuard's behavioral analysis is activated by two events. When a program is launched for the first time, DeepGuard analyses it to determine if it is safe to run. Subsequently, DeepGuard continues to monitor the program while running.

1. Pre-launch analysis

When a program is first executed, regardless of how it is launched (the user clicks the file icon, an e-mail attachment or program initiates it, etc.), DeepGuard temporarily delays it from executing in order to perform the following checks:

1.1 File reputation check

If an Internet connection is available, DeepGuard sends a query to the **Security Cloud** (below) to check for the latest information on the program's reputation in the clean file database, which contains the latest security evaluations for a vast catalog of commonly used applications. This database is maintained and constantly updated by F-Secure Labs analysts. Programs that have been rated as clean in the database are allowed to bypass additional checks and launch immediately, whereas known malicious files are blocked at once.

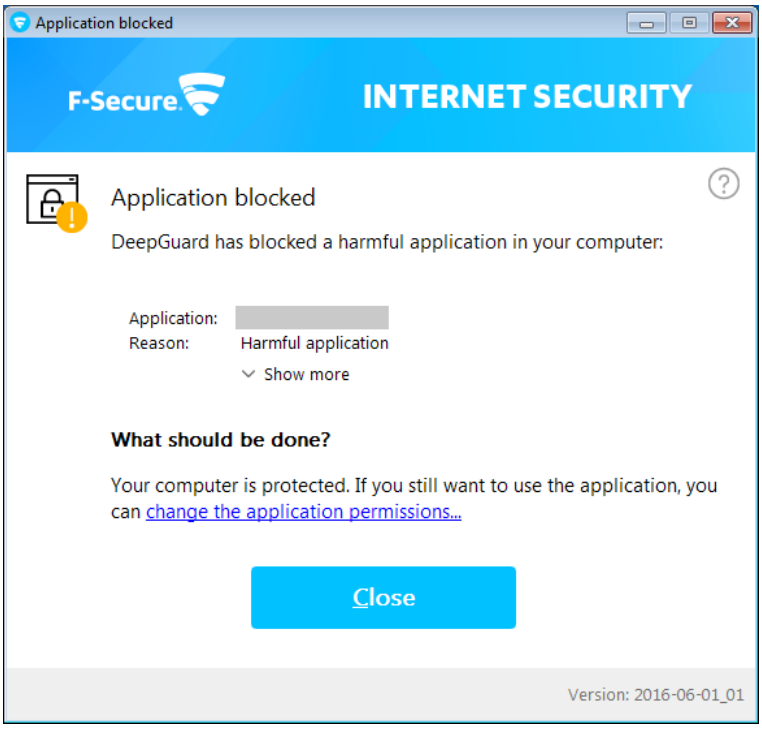
For the user, the clean file cloud lookup functionality offers a number of advantages. Being able to use the security verdict for a known file from the clean file database not only removes the burden of identifying unknown or unfamiliar programs as legitimate or malicious from the user, it also means unnecessary security checks on clean files can be avoided. At the same time, by reducing to a manageable level the volume of software that needs to be individually evaluated, the ability to still white- or black-list selected programs becomes more meaningful.

Security Cloud

In operation since 2008, the Security Cloud (formerly known as the Real-Time Protection Network) is F-Secure's cloud network, housing the various databases and automated analysis systems that support and enhance the performance of F-Secure security products installed on client machines. The infrastructure for this network is hosted on servers in multiple data centers around the world.

Client machines that connect to the Security Cloud are able to retrieve the most up-to-date details of threats seen in the wild by other protected machines, making response far more efficient and effective. When a new object, such as a file or URL, is encountered on one client, the product communicates with the Security Cloud using the strongly encrypted Object Reputation Service Protocol (ORSP) to query for the object's reputation details. Anonymous metadata about the object, such as file size and anonymized path, are sent to the Security Cloud. These queries are completely anonymous

IMAGE: DEEPGUARD BLOCKS A HARMFUL APPLICATION



1.2 Prevalence rate check

DeepGuard includes a module that focuses on a file's prevalence rate. Clean files typically have thousands or millions of users, making them highly prevalent. In contrast, malware samples are comparatively rare.

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

Judgement on execution

Based on the file's reputation and behavior during emulation, DeepGuard makes one of four possible judgements:

A. The file is malicious and blocked
B. The user is given the option to allow or deny the launch
C. The file is clean and allowed to execute
D. The file's status as clean or malicious is still unknown

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

2. During application execution

Even after a program has successfully passed pre-launch analysis and is executed, DeepGuard continues to monitor its behavior as a precaution against delayed malicious routines, a common tactic used by malware to circumvent runtime checks. This form of quiet vigilance also allows DeepGuard to provide constant protection for the user without visibly intruding on their experience by displaying excessive prompts.

and the IP address is not stored, maintaining the client's privacy.

By evaluating the metadata sent, together with information drawn from the in-house databases and various other sources, the Security Cloud's automated analysis systems (which make up to 8 million decisions per day) can provide a fully-informed, up-to-date risk assessment for the object during DeepGuard's pre-launch security evaluation stage, immediately blocking a threat that has been previously seen by any other machine connected to the Security Cloud. This also removes the need to perform further analysis of the object on the client, reducing impact on the user's experience.

The Security Cloud also allows F-Secure Labs analysts to provide critical human intelligence and judgment to complement the automated systems and on-host scanning technology. In addition to creating and maintaining the rules that underpin the databases and automated analysis systems, analysts actively monitor the threat landscape and research malware characteristics and behavior patterns to find the most effective ways to identify truly malicious programs. Once a threat has been confirmed (or a known file's reputation is modified), the updated details take 60 seconds to replicate across all products connected to the Security Cloud, ensuring up-to-date protection.

2.1 Process monitoring

Applications are monitored for a number of suspicious actions, including (but 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 legitimate programs will also perform such actions from time to time, DeepGuard does not red-flag a program on the basis of a single action but instead watches for multiple suspicious operations. Once a critical threshold of suspect actions is reached, DeepGuard will block the process from continuing.

If available, file reputation and prevalence rating information from the Security Cloud is taken into account to determine this critical threshold. For example, DeepGuard treats files with a low-prevalence rating more aggressively by lowering the critical threshold of suspicious actions that can be performed before the file is blocked.

EXPLOIT INTERCEPTION

Starting in 2013, DeepGuard also employs two exploit interception methods that extend the dynamic protection of on-host behavioral analysis by focusing specifically on monitoring the processes of programs that are commonly targeted for exploitation and on document file types commonly used to deliver exploits.

1. Monitoring exploit-prone programs

The first method focuses on frequently exploited programs such as Adobe Flash Player, Microsoft Office, web browsers and so on. These programs are kept under especially close watch and are blocked more aggressively if malicious behavior is detected.

Of course, which programs become favored targets is unlikely to stay fixed. For example, it was only in the last couple years that Adobe's Flash Player superseded Oracle's Java Runtime Environment (JRE) as the most targeted software; in the future, another program may assume that unenviable distinction. The specific programs chosen by DeepGuard for closer attention can be updated by F-Secure Labs analysts when necessary, a responsive approach that allows DeepGuard to adapt to changes in the threat landscape.

2. Monitoring for document exploits

Some document types, such as Microsoft Word or Adobe PDF, are commonly used to deliver exploits. Thus, any software used to open these types of documents is also subject to greater attention by the second exploit interception method, which scrutinizes these programs closely for suspicious behavior caused by malicious document files.

This exploit interception module addresses the most common form of targeted attack, which involves sending carefully crafted, exploit-loaded documents to the intended victim or organization. This was the type of attack carried out by the threat actors behind such campaigns as the 2013 'Red October' campaign [7] and the 2014 attacks against Ukrainian targets reported in our 'BlackEnergy & Quedagh' whitepaper [8].

This type of attack is particularly effective if the exploits used target a zero-day vulnerability. In a more recent example, in 2015 the cyber espionage group known variously as Sofacy, Pawn Storm or APT28 used exploits targeting zero-day flaws in Microsoft Office (CVE-2015-2424) and Java (CVE-2015-2590) in order to install a dropper on the affected machine [9].

In all these cases, booby-trapped document files were used to exploit either known or new vulnerabilities in installed programs. By focusing on detecting malicious actions originating from document files however, Deepguard's exploit interception module is able to provide significant breadth of coverage against document-based exploits, regardless of the file's physical features or the specific vulnerability being targeted.

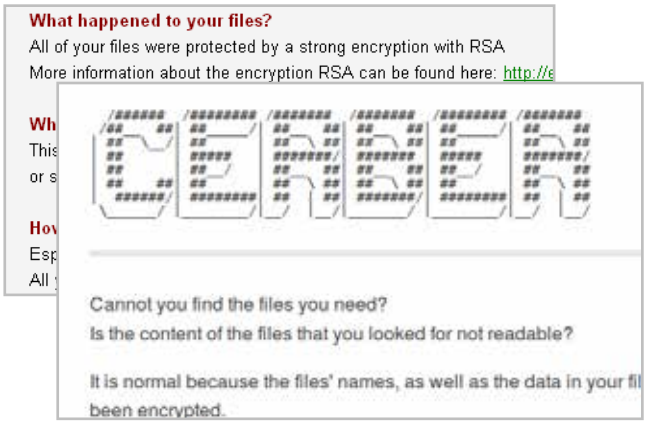
CASE STUDY

DETECTING CRYPTO-RANSOMWARE

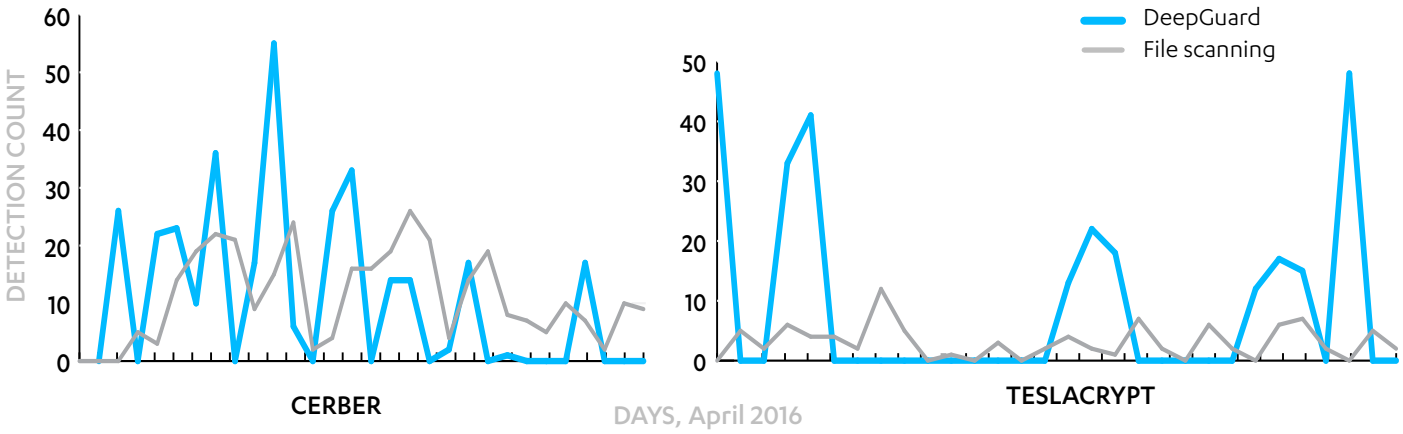
Ransomware is a type of malicious program that uses deceptive and alarming messages to extort money from a victim. **Crypto-ransomware** is a type of ransomware that encrypts files stored on the user's computer or mobile device, essentially taking them hostage. A ransom demand (right) is then shown to the user demanding payment for a decryption key that can be used to restore the affected files. Because the encryption used to 'scramble' the files is usually extremely difficult to break, crypto-ransomware infections can be severely disruptive, especially if they successfully infect computers in major corporations or organizations such as hospitals [10].

Like any other malware however, crypto-ransomware exhibits characteristic behavior that betrays its nature, making it possible for DeepGuard to spot and intercept the threat.

IMAGE: RANSOM DEMANDS MADE BY CERBER & TESLACRYPT CRYPTO-RANSOMWARE



DETECTION COUNT REPORTED BY CLIENTS FOR CERBER & TESLACRYPT CRYPTO-RANSOMWARE, APRIL 2016



Detecting crypto-ransomware behavior

We can best see DeepGuard in action against crypto-ransomware by looking at the telemetry data reported by machines with installed F-Secure products (also known as *clients*). In the charts above, we track the count of detections reported by clients in April 2016 for the **Cerber** and **TeslaCrypt** crypto-ransomware families. The count of detections are divided between those reported by the DeepGuard component in the clients, and those from the file scanning engines.

The charts demonstrate DeepGuard's effectiveness in identifying and blocking the malware, in many cases being the first component to do so. This is best seen in the chart for TeslaCrypt, where DeepGuard was clearly responsible for the majority of the detections reported. Especially for new variants of these ransomware families, DeepGuard was the last and best line of defense preventing them from infecting the machines.

While DeepGuard kept the clients directly protected, the other elements of F-Secure's multi-layered security approach were active in other ways. The first clients that encountered the ransomware shared their details to the Security Cloud, giving all other connected clients advance warning and effectively 'immunizing' them against a threat they had not yet encountered. It also allowed F-Secure Labs analysts to update the file scanning engines. As they started detecting the malware before DeepGuard could be triggered, detection counts for the engines increased while those for DeepGuard declined, as expected.

This data from real-world clients illustrates how DeepGuard's on-host behavioral analysis effectively counters even severe threats such as crypto-ransomware. In addition, by using DeepGuard in tandem with the other components in a multi-layered security strategy, F-Secure products can share critical details so that all clients are protected against even the latest threats.

FALSE POSITIVE PREVENTION

A separate beta detections module that was added to DeepGuard in 2011 facilitated an understated but important improvement to the accuracy of the scanning engine's performance.

Beta detections contain the full detection logic needed to identify and block exploit attempts, but are instead configured by F-Secure Labs analysts to simply notify the Security Cloud each time the detection would have been triggered by a file being analyzed.

This beta-testing process provides F-Secure Labs analysts with crucial information on the effectiveness of these detections, allowing them to fine-tune the logic to prevent potential false positives before actually releasing them for real-world use.

CONCLUSION

F-Secure's security products use a multi-tiered 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 are able to analyze and issue a detection for that specific threat.

Through lookups to F-Secure'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 also extends to intercepting attacks attempting to exploit vulnerabilities in popular programs in order to install malware onto the machine. DeepGuard is able to identify and block routines 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 combines sophisticated scanning engine technology with the technical expertise of F-Secure Labs analysts to perform accurate, fine-grained on-host behavior- and reputation-based analysis that ultimately significantly improves the user's security.

References

1. F-Secure Labs: *Article: Crypto-ransomware*; https://www.f-secure.com/en/web/labs_global/crypto-ransomware
2. Federal Bureau of Investigation; *Public Service Announcement: Criminals Continue to Defraud and Extort Funds from Victims Using CryptoWall Ransomware Schemes*; published Jun 23 2015; http://www.ic3.gov/media/2015/150623.aspx
3. F-Secure Labs Threat Description: *Worm:W32/Downadup*; https://www.f-secure.com/v-descs/worm_w32_downadup.shtml
4. F-Secure Labs Threat Description: *Virus:W32/Sality*; https://www.f-secure.com/v-descs/virus_w32_sality.shtml
5. AV-TEST; *AV-Test Award 2012*; published 28 Jan 2013; http://www.av-test.org/en/test-procedures/award/2012/

Availability

DeepGuard is an integral component of various F-Secure 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 also be turned off separately.

6. F-Secure Weblog; *What's The Deal With Prevalence*; published 8 Jun 2016; https://labsblog.f-secure.com/2016/06/08/whats-the-deal-with-prevalence/
7. F-Secure Weblog; *Every Month is Red October*; published 15 Jan 2013; http://www.f-secure.com/weblog/archives/00002486.html
8. F-Secure Weblog; *BlackEnergy 3: An Intermediate Persistent Threat*; published 25 Sep 2014; https://www.f-secure.com/weblog/archives/00002747.html
9. F-Secure Weblog; *Sofacy Recycles Carberp and Metasploit Code*; published 8 Sep 2015; https://labsblog.f-secure.com/2015/09/08/sofacy-recycles-carberp-and-metasploit-code/
10. Arstechnica; Sean Gallagher; *Hospital pays $17k for ransomware crypto key*; published 18 Feb 2016; http://arstechnica.com/security/2016/02/hospital-pays-17k-for-ransomware-crypto-key/


F-Secure.