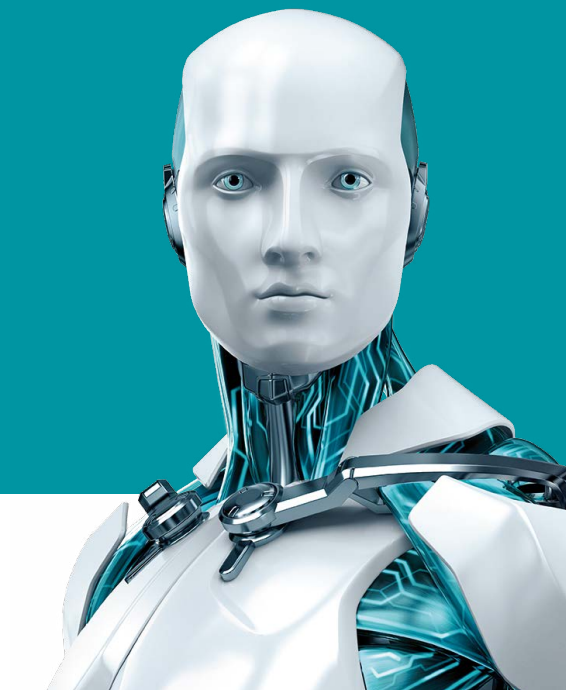
ESET TECHNOLOGIE

Setzt Maßstäbe in Sicherheit und Performance

Autoren:
Jakub Debski, Chief Product Officer
Juraj Malcho, Chief Technology Officer
Peter Stančík, Security Research and Awareness Manager

Dokumentversion: 1.3



ENJOY SAFER TECHNOLOGY™

INHALTSVERZEICHNIS

ZIELE

In diesem Dokument erklären wir, inwiefern ESETs vielschichtige Sicherheitstechnologien weit mehr bieten als reinen Virenschutz. Erfahren Sie, wann Bedrohungen auf einem System durch welche Schutzmodule erkannt bzw. blockiert werden und welche Vorteile sich für Nutzer ergeben.

SICHERHEITSLÖSUNGEN DER NÄCHSTEN GENERATION?

Die meisten etablierten Antiviren-Unternehmen wurden mit dem Ziel gegründet, Internetnutzern bei der Bewältigung ihrer Probleme mit Viren und anderen Schädlingen zu helfen. Mit zunehmender Vielfalt ernster Bedrohungen wurden auch immer komplexere Schutztechnologien entwickelt. Heute ist IT-Sicherheit eine etablierte Branche am Markt und ein Thema, das jeden betrifft – unabhängig davon, ob man wirklich versteht, worum es hierbei geht. Neuerdings entstehen immer mehr Startups, die sich selbst als Unternehmen der „nächsten Generation" bezeichnen. In der Regel haben sie weniger Erfahrung in der Entwicklung von Sicherheitslösungen, vermarkten sie aber offensiv als „innovativ" und stempeln etablierte Hersteller als „Dinosaurier" ab. Ironischerweise verlassen sie sich jedoch bei ihrer Erkennungsleistung oftmals auf die Technologien bekannter Hersteller, da nur wenige Lösungsanbieter die Erfahrung und Kapazität haben, ihre eigenen Kernmodule zu entwickeln. Alle ESET Technologien sind urheberrechtlich geschützt und wurden intern entwickelt.

Die einfache Erkennung durch statische Signaturen, die – laut der Newcomer – die Effektivität etablierter Lösungsanbieter einschränkt, ist mittlerweile nur noch eine kleine Komponente der Technologien, die in einem modernen Sicherheitsprodukt zum Schutz vor aktuellen Bedrohungen eingesetzt werden.

VIELSCHICHTIGER SCHUTZ VOR VIELFÄLTIGEN BEDROHUNGEN

Die „alten Hasen" der Antiviren-Branche sind deshalb auch heute noch im Geschäft, weil sie ihre Schutzmechanismen immer wieder den sich stets wandelnden Gefahren angepasst haben.

Heutige Bedrohungen lassen sich nicht mit Technologien aus den 90er Jahren abwehren. Der Kampf gegen moderne Malware ist ein Katz-und-Maus-Spiel gegen begabte und (finanziell) motivierte Cybergangster. So müssen Sicherheitsunternehmen ihre Produkte sowohl hinsichtlich proaktiver als auch reaktiver Schutzmaßnahmen stets weiterentwickeln, damit auch neuartige Malware zuverlässig erkannt und blockiert wird. Ein einzelner Ansatzpunkt oder Verteidigungsmechanismus reicht bei weitem nicht aus.

Aus diesem Grund hat sich ESET von einem einfachen Antiviren-Hersteller zu einem umfassenden IT-Sicherheitsanbieter entwickelt.

Plattformübergreifende Bedrohungen

Microsoft Windows ist nicht die einzige Plattform, die von Malware betroffen ist. Angreifer sind immer darum bemüht, auch bislang unerschlossene Plattformen und Prozesse für ihre Zwecke zu missbrauchen und schaffen dadurch ein immer größeres Kampfgebiet. Hierbei gilt:

- Alles, was für die Durchführung schädlicher Aktivitäten genutzt werden kann, ist für Angreifer ein lohnendes Ziel.
- Alles, was zur Verarbeitung von externen Daten einen ausführbaren Code startet, kann von schädlichen Daten missbraucht werden.

Linux Server sind ein beliebtes Angriffsziel (Operation Windigo, *Linux/Mumblehard*), eines der bisher größten Botnets (*OSX/Flashback*) wurde auf Mac OS X-Rechnern gehostet, immer häufiger werden Mobiltelefone

angegriffen (*Hesperbot*) und Attacken gegen Router entwickeln sich zu einer zunehmend ernsten Bedrohung (*Linux/Moose*). Rootkits kommen der Hardware immer näher (Angriffe auf Firmware oder Nutzung des *UEFI-Rootkits*) und der zunehmende Einsatz von Virtualisierung eröffnet neue Angriffsvektoren (Bluepill, VM-Escape-Schwachstellen). Webbrowser und andere Anwendungen sind mittlerweile genauso komplex wie Betriebssysteme und ihre Skripting-Mechanismen werden häufig für schädliche Zwecke missbraucht (*Win32/Theola*).

Viele Wege führen aufs System

Die erste Malware war ein sich selbst replizierender Prozess, der sich zunächst innerhalb von Systemen, dann als Datei- und/oder Festplatten-infizierender Virus von PC zu PC ausbreitete. Durch das Internet haben allerdings die Infektionsmöglichkeiten deutlich zugenommen.

So können schädliche Objekte als Anhang oder Links in E-Mails, über Skripte in einem Dokument, als Download auf Webseiten oder über externe Speichergeräte auf ein System eingeschleust werden. Darüber hinaus nutzen Kriminelle schwache Anmeldeverfahren und Passwörter sowie Sicherheitslücken in Anwendungen aus oder versuchen, den Nutzer mithilfe von Social Engineering zur Installation des Schädlings zu bringen.

Malware-Design

Die Zeiten, in denen Malware vorrangig aus Spaß von computerbegeisterten Teenagern geschrieben wurde, sind lange vorbei. Heutzutage geht es den Malware-Autoren um Geld und Informationen. Es wird eine Menge in die Entwicklung investiert – sowohl von Kriminellen als auch von Regierungen.

Mit dem Ziel, die Erkennung zu erschweren, werden die Schädlinge in unterschiedlichen Programmiersprachen mit verschiedenen Compilern und interpretierten Sprachen entwickelt. Darüber hinaus wird der schädliche Code mithilfe spezieller Software getarnt und verschlüsselt. Er wird in saubere Prozesse eingeschleust, um bei einer verhaltensbasierten Prüfung – bei der auffällige Aktivitäten erkannt werden – keine Aufmerksamkeit zu erregen und möglichst lange unentdeckt auf dem System zu verweilen. Mit Skripten werden Techniken zur Anwendungskontrolle umgangen und zum Schutz vor Datei-basierten Sicherheitsmechanismen wird Malware oftmals ausschließlich im Arbeitsspeicher ausgeführt.

Die Kriminellen fluten das Internet mit Tausenden an Malware-Varianten, um ihren Erfolg sicherzustellen oder greifen nur vereinzelte Ziele an, um von Sicherheitsunternehmen unentdeckt zu bleiben. Sie missbrauchen Softwarekomponenten zur Säuberung oder signieren den schädlichen Code mit Zertifikaten, die sie von legitimen Unternehmen stehlen, wodurch eine Erkennung abermals erschwert wird.

Auf Netzwerkebene macht Malware immer weniger Gebrauch von hartkodierten Command and Control (C&C) Servern, um Befehle zu erhalten und Daten von den kompromittierten Systemen zu übermitteln. Zunehmend werden Botnets mithilfe von Peer-to-Peer-Netzwerken dezentralisiert gesteuert. Durch die Verschlüsselung der Kommunikation wird die Identifizierung von Angriffen zusätzlich erschwert. Mit dem Einsatz von Domain-Generation-Algorithmen verliert die Erkennung auf Basis der Blockierung als schädlich bekannter URLs an Effektivität.

Angreifer übernehmen die Kontrolle über legitime Webseiten mit gutem Ruf oder nutzen legale Webdienste, um schädliche Inhalte zu platzieren.

WICHTIGER HINWEIS
Die Angreifer nutzen viele Tricks, um eine Erkennung zu verhindern. Simple Lösungen reichen hier schon lange nicht mehr aus, um zuverlässige Sicherheit zu gewährleisten. Für maximalen Schutz setzen wir von ESET deshalb auf einen konstanten, vielschichtigen Echtzeit-Schutz.

STARKE TECHNOLOGIE VON ESET

Kern all unserer Produkte ist die ESET Scan Engine. Während die zugrundeliegende Technologie ihren Ursprung im „Antivirus der alten Schule“ hat, wurde sie über die Zeit immer wieder erweitert und verbessert, um auch moderne Bedrohungen zuverlässig abzuwehren.

Die Scan Engine soll potenzielle Bedrohungen erkennen und automatisch entscheiden, ob sie tatsächlich schädlich sind.

Über viele Jahre hinweg basierte ESETs Performance auf intelligenten Algorithmen und manuell erstellten Assembler-Codes. Hiermit sollten Leistungsengpässe bewältigt werden, die durch die Tiefenanalyse eines Codes mithilfe der im Produkt integrierten Sandboxing-Technologie verursacht wurden. Mittlerweile haben wir den Ansatz allerdings verbessert und nutzen binäre Übersetzungen zusammen mit interpretierter Emulation, um maximale Performance zu gewährleisten.

Bei der Sandboxing-Methode werden verschiedene Hard- und Softwarekomponenten nachgebildet, um ein Programm in einer virtualisierten Umgebung auszuführen. Zu diesen Komponenten gehören Speicher, Dateisystem, Betriebssystem, APIs und die CPU (Central Processing Unit).

Früher wurde die CPU mithilfe eines speziellen Assembler-Codes nachgebildet. Allerdings handelte es sich hierbei um einen „interpretierten Code“, wobei jede Anweisung separat nachgeahmt werden musste. Mit binärer Übersetzung werden diese Anweisungen nativ auf einer echten CPU ausgeführt. Diese Methode beschleunigt insbesondere die Analyse von Codes mit Schleifen: Solche Schleifen werden häufig in ausführbaren Dateien genutzt, in denen Maßnahmen zum Schutz vor einer Analyse durch Sicherheitslösungen und Researcher implementiert sind.

ESET Produkte analysieren Hunderte verschiedene Dateiformate (ausführbare Dateien, Installer, Skripte, Archive, Dokumente und Bytecodes), um eingebettete schädliche Komponenten zuverlässig zu erkennen.

Die folgende Abbildung beinhaltet die verschiedenen Kerntechnologien von ESET und zeigt, wann Bedrohungen auf einem System erkannt und/oder blockiert werden.

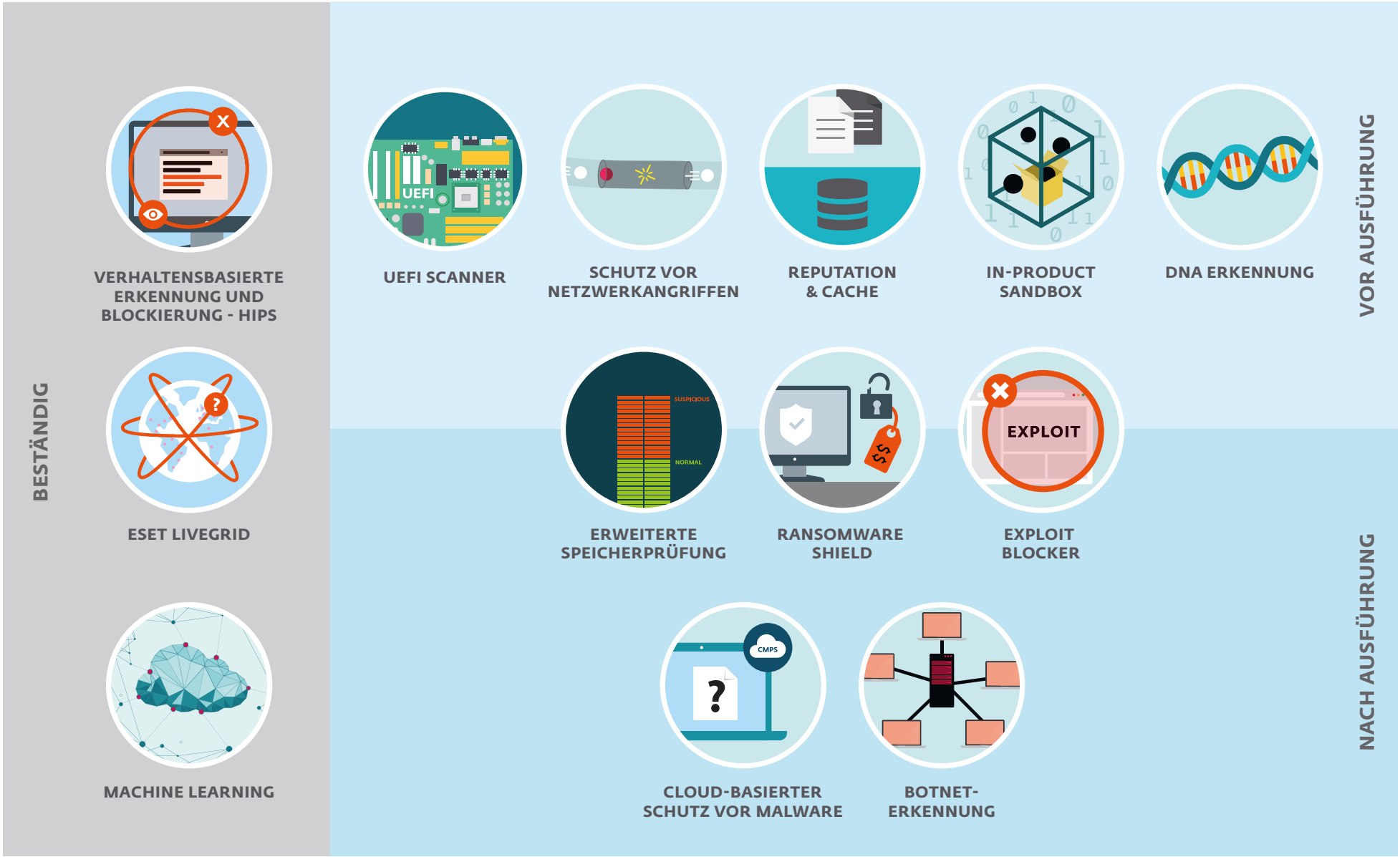
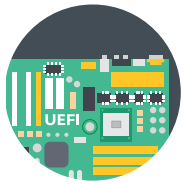


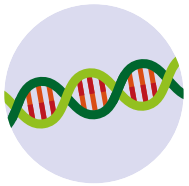
Abb. 1: Schutzschichten der ESET Technologie



UEFI-Scanner

ESET ist der erste IT Security Anbieter, der einen Mechanismus zum Schutz des Unified Extensible Firmware Interface (UEFI) implementiert hat. Der UEFI-Scanner prüft Systeme mit UEFI-Bootumgebung und gewährleistet dadurch die Sicherheit und Integrität der Firmware. Bei Auffälligkeiten wird der Nutzer umgehend informiert.

UEFI ist eine Standardspezifikation der Softwareschnittstelle zwischen Betriebssystem und Firmware eines Geräts. Es ist der Nachfolger des Mitte der 1970er Jahre eingeführten Basic Input/Output Systems (BIOS). Dank des gut dokumentierten Aufbaus kann UEFI leichter analysiert und aufgegliedert werden, sodass Entwickler Erweiterungen für die Firmware erstellen können. Allerdings bedeutet das zugleich, dass es auch Malware-Autoren und Angreifer leichter haben, die Schnittstelle mit ihren schädlichen Modulen zu infizieren.



DNA Erkennung

Die ESET Scan Engine erkennt schädliche Objekte anhand verschiedener Kriterien. Der eindeutige „Fingerabdruck“ (Hash) ist besonders nützlich bei der Erkennung spezieller Malware-Versionen, bei der Erstellung von Statistiken oder der genaueren Bestimmung von Erkennungsnamen für bekannte Malware. Die sogenannten DNA Erkennungen basieren auf komplexen Definitionen von Verhaltensmustern und anderen Malware-Charakteristika.

Der Musterabgleich durch klassische Antiviren-Produkte kann mithilfe einfacher Modifikationen des Codes oder durch den Einsatz von Verschleierungstechniken umgangen werden. Das Verhalten eines schädlichen Objekts lässt sich allerdings nicht so leicht verändern.

Genau hier greifen die DNA Erkennungen von ESET. Bei der Tiefenanalyse eines Codes werden die für das Verhalten verantwortlichen Teile extrahiert. Diese beinhalten weit mehr Informationen als die sogenannten Indicators of Compromise (IOCs), die manche Anbieter der „nächsten Generation“ als bessere Alternative zur Signaturerkennung bezeichnen. Die für das Verhalten verantwortlichen Teile werden genutzt, um eine DNA Erkennung zu erstellen, mit deren Hilfe potenziell schädliche Codes erkannt werden, die ein ähnliches Verhalten zeigen.

Darüber hinaus extrahiert unsere Scan Engine viele weitere ausschlaggebende Bestandteile, die der Erkennung von Abweichungen dienen.

Je nach eingestellten Schwellenwerten und Bedingungen für den Abgleich identifizieren DNA Erkennungen bekannte Schädlinge, neue Varianten bekannter Malware-Familien oder sogar bislang unbekannte Bedrohungen anhand ihres schädlichen Verhaltens. So können mit einer guten DNA Erkennung Zehntausende Malware-Varianten entdeckt werden.

Zudem ermöglichen die automatische Erstellung von Clustern sowie die Anwendung von Machine Learning Algorithmen unserer Scan Engine, neue schädliche Bestandteile und Verhaltensmuster zu erkennen. Diese Komponenten können mit Whitelists abgeglichen werden, um Fehlalarme zu verhindern.

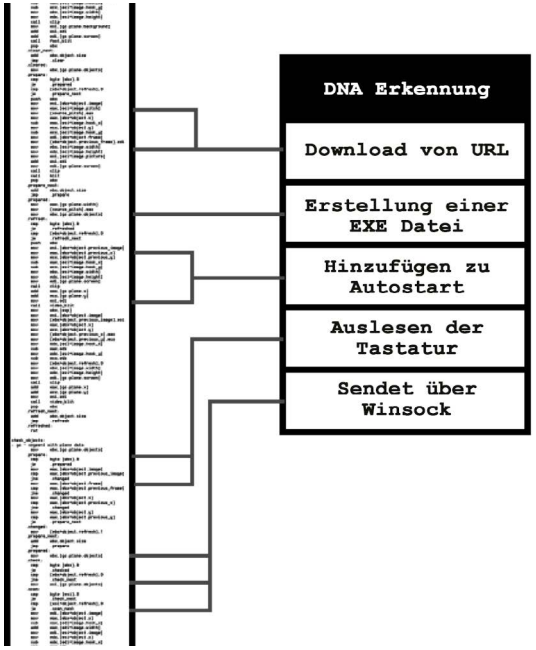


Abb. 2: Beispiel einer DNA Erkennung

Machine Learning

ESET testet bereits seit den 1990er Jahren den Einsatz von Machine Learning Algorithmen zur Abwehr von Bedrohungen. Seit 1998 sind neuronale Netzwerke Bestandteil unserer Produkte und ein wichtiger Baustein unseres mehrschichtigen Sicherheitskonzepts.

So nutzen auch DNA Erkennungen auf Machine Learning basierende Modelle, um mit oder ohne Verbindung zur Cloud effektiv zu arbeiten. Darüber hinaus werden Machine Learning Algorithmen bei der ersten Sichtung und Klassifizierung eingehender Samples sowie deren Platzierung auf der imaginären „Cybersicherheits-Landkarte" genutzt.

Die Machine Learning Engine namens „Augur" wurde eigens von ESET entwickelt. Die Technologie nutzt eine Kombination aus neuronalen Netzwerken (wie Deep Learning und Long short-term memory) und sechs Klassifizierungsalgorithmen. Das ermöglicht eine zuverlässige Einstufung von eingehenden Samples als sicher, potenziell unerwünscht oder schädlich.

ESET Augur arbeitet reibungslos mit den anderen Schutzmechanismen wie DNA Erkennung, Sandboxing und Speicherprüfung sowie der Extrahierung von Verhaltensmerkmalen zusammen, um eine maximale Erkennungsrate bei minimalen Fehlalarmen zu gewährleisten.

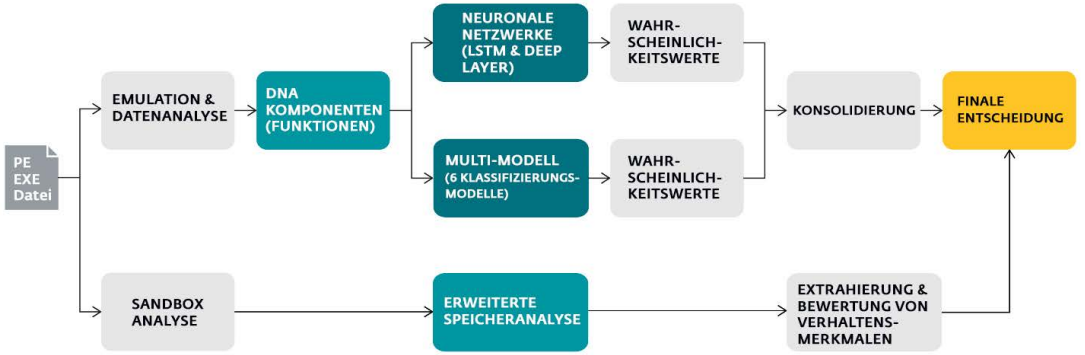


Abb. 3: Schema der ESET Machine Learning Engine Augur

ESET LiveGrid

Der einfachste Weg, mit einem Cloudsystem Schutz zu bieten, besteht in zuverlässigem Blacklisting mithilfe von Hashes. Hierdurch werden schädliche Dateien und URLs erkannt und blockiert, allerdings nur dann, wenn sie genau mit dem Hash übereinstimmen. Diese Einschränkung hat zur Entwicklung des so-genannten „Fuzzy Hashing" geführt, bei dem auch Ähnlichkeiten zwischen zwei Objekten berücksichtigt werden.

ESET hat das Fuzzy Hashing weiterentwickelt. Wir führen kein Hashing von Daten durch, sondern von dem in der DNA Erkennung beschriebenen Verhalten. Mithilfe des DNA Hashings können wir umgehend Tausende unterschiedliche Malware-Varianten blockieren.

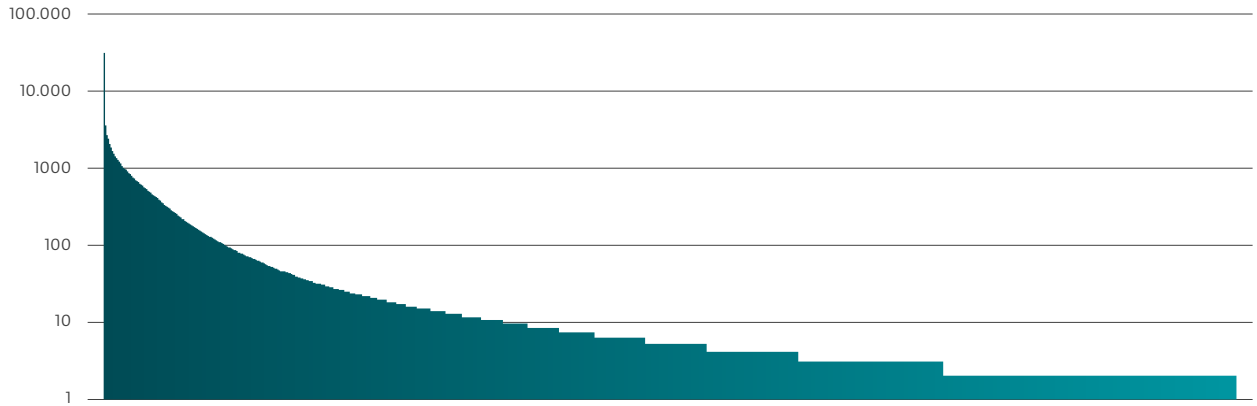


Abb. 4: Anzahl an eindeutigen Dateien (y-Achse), die durch individuelle DNA Hashes (x-Achse) erkannt werden.

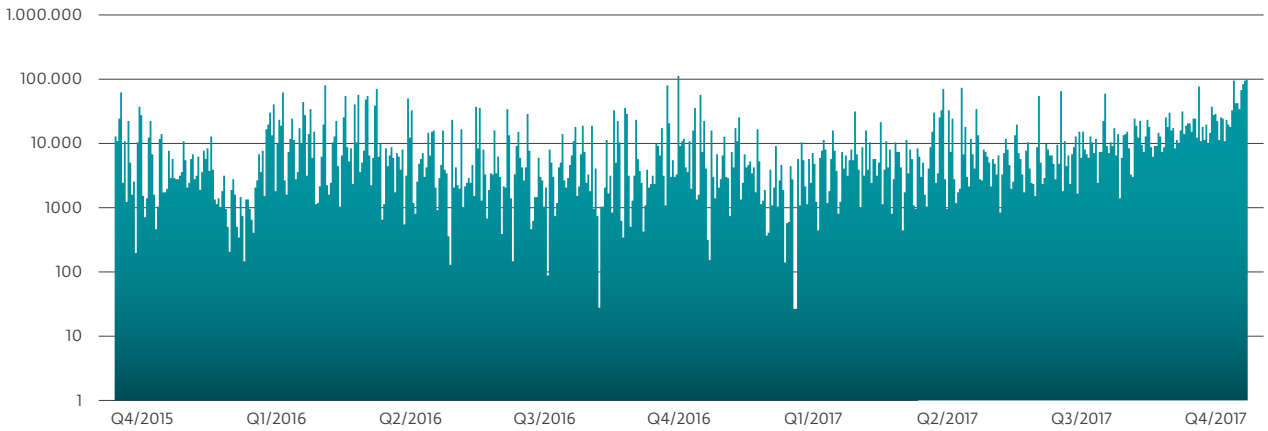


Abb. 5: Anzahl an eindeutigen Dateien (y-Achse), die täglich durch DNA Hashes (x-Achse) erkannt werden.

Cloudbasierter Schutz vor Malware

Wie viele ESET Technologien basiert auch der Cloudbasierte Schutz vor Malware auf dem ESET Cloudsystem LiveGrid. Unbekannte, potenziell schädliche Anwendungen und Bedrohungen werden geprüft und über das LiveGrid Feedback-System an die ESET Cloud eingereicht. Hier werden die gesammelten Samples in einer Sandbox einer verhaltensbasierten Analyse unterzogen. Wird ein Sample als schädlich bewertet, wird automatisch eine Erkennung erstellt und noch vor dem nächsten Update der Detection Engine über das ESET LiveGrid Reputationssystem unseren Kunden zur Verfügung gestellt. Die Bearbeitungszeit des Mechanismus liegt unter 20 Minuten. So ist der Nutzer bereits vor der Aktualisierung der Detection Engine vor neuaufkommenden Bedrohungen geschützt.

Je mehr Nutzer sich entscheiden, die Einreichung von Samples mit fragwürdiger Reputation zur Tiefenanalyse bei ESET zuzulassen, desto effektiver arbeitet der Cloudbasierte Schutz vor Malware.

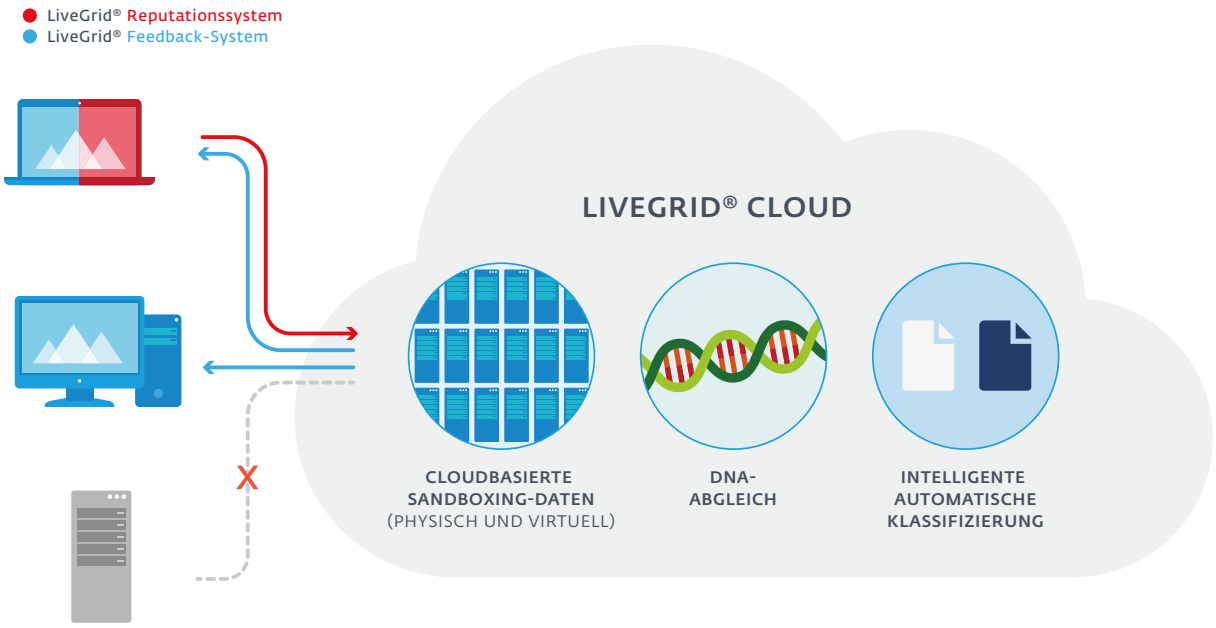


Abb. 6: ESETs Cloudbasierter Schutz vor Malware

Reputation & Cache

Vor der Prüfung von Dateien oder URLs fragen unsere Produkte beim lokalen Cache (im Falle der ESET Endpoint Security auch beim ESET Shared Local Cache) an, ob das Objekt bereits als schädlich oder sicher eingestuft wurde. Hierdurch werden unnötige Mehrfachscans ungefährlicher Objekte vermieden.

Anschließend wird der eindeutige „Fingerabdruck" (Hash) des Objekts mit der Reputationsdatenbank ESET LiveGrid® abgeglichen. Hierbei wird ermittelt, ob das Objekt schon irgendwo anders aufgetaucht und als schädlich bekannt ist. Dies steigert die Effektivität der Prüfung und ermöglicht zudem eine schnellere Bereitstellung wichtiger Informationen über aktuelle Bedrohungen.

Mithilfe von URL-Blacklisting sowie der Prüfung der Reputation werden Nutzer vor Webseiten mit schädlichen Inhalten geschützt.

Verhaltensbasierte Erkennung – HIPS

ESETs hostbasierter Schutz vor Angriffen (HIPS) beobachtet die Systemaktivitäten und erkennt verdächtiges Systemverhalten anhand vordefinierter Regeln. Werden solche Aktivitäten identifiziert, verhindert der Selbstschutzmechanismus des Moduls die Ausführung der entsprechenden Programme oder Prozesse. Nutzer können neben den vordefinierten Regeln auch ein eigenes Regelwerk erstellen, allerdings erfordert dies erweiterte Kenntnisse über Anwendungen und Betriebssysteme.

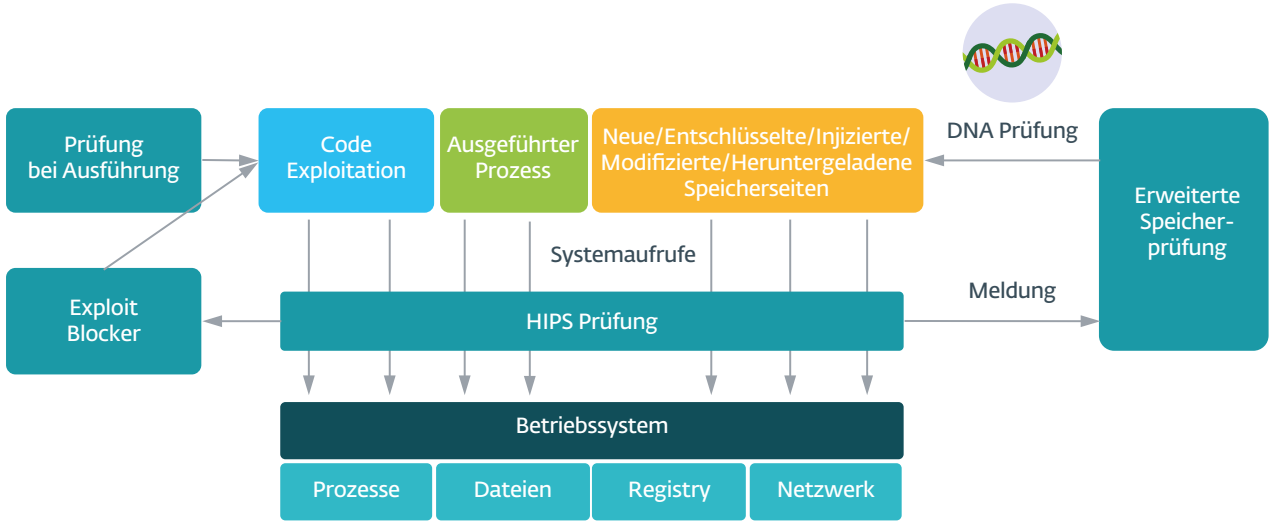
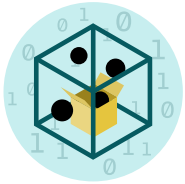


Abb. 7: Funktionsweise der Verhaltensbasierten Erkennung



Im Produkt integrierte Sandbox

ESET hat die DNA Erkennung in zwei Teile gegliedert, um den ganzen Prozess besser nachvollziehen zu können. Diese Idee hatten wir 1995, als wir erstmals einen Emulator in unseren Produkten einsetzten. Damit extrahieren wir Metadaten über das Verhalten eines Samples, die zur Erstellung der DNA Erkennungen genutzt werden. So decken wir das tatsächliche Verhalten einer getarnten Malware auf, die einer Erkennung zu entgehen versucht. Dabei kommen zudem binäre Übersetzungen zum Einsatz, sodass durch das im Produkt integrierte Sandboxing keine Leistungsengpässe verursacht werden.

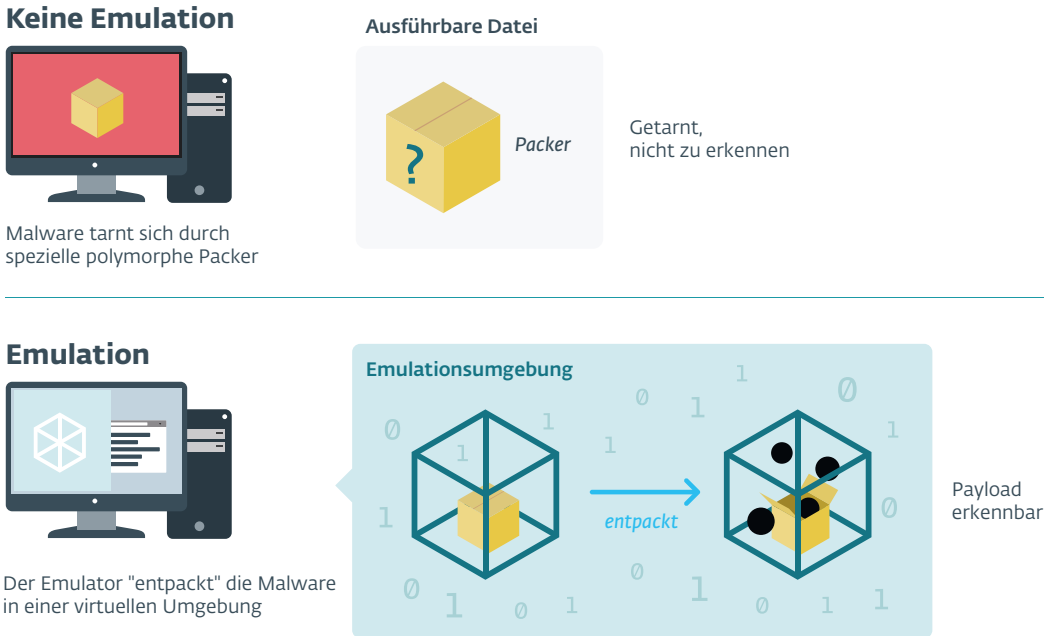
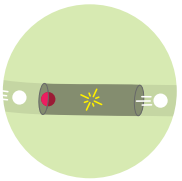
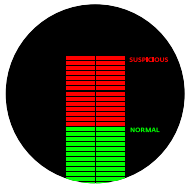


Abb. 8: Weshalb ESET im Produkt integriertes Sandboxing verwendet



Schutz vor Netzwerkangriffen

Der Schutz vor Netzwerkangriffen ist eine Erweiterung der Firewall und verbessert die Erkennung bekannter Schwachstellen auf Netzwerkebene. Durch die Implementierung der Erkennung gängiger Schwachstellen in häufig genutzten Protokollen wie SMB, RPC und RDP bietet dieses Modul einen zuverlässigen Schutz vor Malware und Angriffen, die über Netzwerke verbreitet werden, sowie vor Ausnutzungsversuchen von Schwachstellen, für die noch kein Patch veröffentlicht oder bereitgestellt wurde.



Erweiterte Speicherprüfung

Die Erweiterte Speicherprüfung ist eine einzigartige ESET Technologie, die auf ein wichtiges Problem bei der Abwehr moderner Malware eingeht – die Tarnung und/oder Verschlüsselung von Schädlingen.

Solche Schutzmechanismen der Malware verursachen Schwierigkeiten für Erkennungsansätze, bei denen Entpackungstechniken wie Emulation oder Sandboxing zum Einsatz kommen. Denn in beiden Fällen besteht keine Garantie dafür, dass die Malware während der Analyse ihr schädliches Verhalten offenbart.

Manche Tarnmechanismen führen dazu, dass nicht alle Ausführungspfade analysiert werden können. So kann die Malware weitere Komponenten nachladen oder Trigger enthalten, durch die der schädliche Code nur unter bestimmten Bedingungen oder zu konkreten Zeiten ausgeführt wird. Die Erweiterte Speicherprüfung wehrt diese Bedrohungen ab, indem sie verdächtige Prozesse enttarnt und blockiert, sobald sie im Arbeitsspeicher ihre schädlichen Funktionen zur Ausführung bereitstellen. Hierdurch werden klassische Erkennungsansätze der proaktiven Code-Analyse vor oder während der Ausführung ergänzt.

Auch zuvor saubere Prozesse können durch Missbrauch oder Code-Injektion plötzlich schädlich werden. Eine einmalige Überprüfung ist also nicht ausreichend. Deshalb behält die Erweiterte Speicherprüfung die Prozesse konstant im Blick. **Startet ein Prozess einen Systemaufruf, analysiert sie mithilfe der DNA Erkennungen das Verhalten des Codes.**

Darüber hinaus schützt die Erweiterte Speicherprüfung vor schädlichen Codes, die keine dauerhafte Komponente im Dateisystem benötigen und ausschließlich im Arbeitsspeicher ausgeführt werden.

Ursprünglich tauchte solche Malware nur auf Servern auf, weil diese über Monate oder gar Jahre hinweg angeschaltet bleiben und schädliche Prozesse auf unbestimmte Zeit im Speicher vorhanden sein können, ohne einen Neustart überleben zu müssen. Allerdings überträgt sich der Trend nun auch auf Endpoints.

Die Code-Analyse wird sowohl für Standardspeicher von ausführbaren Dateien als auch für .NET MSIL (Microsoft Intermediate Language) Code durchgeführt, der von Malware-Autoren genutzt wird, um eine dynamische Analyse zu erschweren. Dank Smart Caching kommt es hierbei zu keinerlei spürbaren Geschwindigkeitseinbußen.

Die Erweiterte Speicherprüfung und der Exploit Blocker ergänzen sich gegenseitig. Bei der Erweiterten Speicherprüfung handelt es sich jedoch um eine reaktive Schutzmethode, die erst nach der Ausführung greift. Es besteht also das Risiko, dass schädliche Aktivitäten bereits auf das System gelangen konnten. Allerdings handelt es sich um **ein letztes Mittel, das nur dann zum Einsatz kommt, wenn die Angreifer alle anderen Schutzmodule umgehen konnten.**

Exploit Blocker

Während die ESET Scan Engine Exploits in manipulierten Dateien abwehrt und der Schutz vor Netzwerkangriffen die Kommunikationsebene absichert, stoppt der Exploit Blocker die Aktionen der Schadsoftware selbst.

Dazu beobachtet der Exploit Blocker konstant das Verhalten häufig angegriffener Anwendungen wie Webbrowser, PDF-Reader, E-Mail-Programme, Flash oder Java. Anstatt sich nur auf bestimmte CVE-Kennungen zu beschränken, werden gängige Ausnutzungstechniken berücksichtigt.

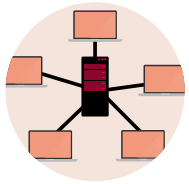
Jeder Exploit ist eine Abweichung zur regulären Ausführung eines Prozesses und wird dadurch als verdächtig erkannt. Die Technologie wird stets weiterentwickelt, um auch neuartige Ausnutzungsmechanismen identifizieren zu können. Wird ein Prozess als auffällig erkannt, wird dessen Verhalten analysiert und umgehend als potenzielle Bedrohung auf der Maschine blockiert. Hierbei werden Metadaten über den Angriff an unser Cloudsystem ESET LiveGrid gesendet.

Mithilfe dieser anonymen Informationen können zuvor unbekannte Bedrohungen wie sogenannte Zero-Day-Angriffe erkannt und die aktuelle Bedrohungslage analysiert werden.

Der Exploit Blocker unterscheidet sich grundlegend von anderen Erkennungstechnologien, die sich auf die Analyse des schädlichen Codes selbst konzentrieren und sorgt dadurch für zusätzlichen Schutz.

Ransomware Shield

Das ESET Ransomware Shield ist eine zusätzliche Schutzschicht, die Nutzer vor Verschlüsselungstrojanern bzw. Erpressermalware bewahrt. Die Technologie überprüft alle ausgeführten Anwendungen und bewertet sie anhand ihres Verhaltens und ihrer Reputation. Werden Prozesse identifiziert, die typisches Ransomware-Verhalten aufweisen oder versuchen, unerwünschte Änderungen an bestehenden Dateien (z.B. Verschlüsselung) vorzunehmen, wird der Nutzer umgehend informiert. Er hat dann die Möglichkeit, die Aktivität zu blockieren. Zusammen mit anderen Technologien wie dem Cloudbasierten Schutz vor Malware, der DNA Erkennung und dem Schutz vor Netzwerkangriffen gewährleistet diese Technologie eine zuverlässige Abwehr von Ransomware.



Botnet-Erkennung

Die Kommunikation zwischen Malware und C&C Servern lässt sich nicht ohne weiteres modifizieren.

Die Botnet-Erkennung identifiziert diese schädliche Kommunikation und gleichzeitig den angreifenden Prozess.

ESETs Netzwerk-Erkennungen erweitern diese Technologie, um schädlichen Netzwerkverkehr noch schneller und zuverlässiger zu erkennen. Mit standardisierten Signaturen wie Snort und Bro werden viele Angriffe entdeckt, doch ESETs Netzwerk-Erkennungen wurden speziell zur Identifizierung von Netzwerk-Schwachstellen, Exploit-Kits und der Kommunikation besonders raffinierter Malware entwickelt.

Die Analyse des Netzwerkverkehrs auf Endpoints hat weitere Vorteile. So kann der für die schädliche Kommunikation verantwortliche Prozess oder das entsprechende Modul identifiziert werden. Hierdurch können umgehend Aktionen zum Schutz vor dem infizierten Objekt eingeleitet und manchmal sogar die Verschlüsselung der Kommunikation umgangen werden.

Botnet-Tracker

Wird ein Sample oder dessen Speicherauszug von ESETs Systemen als Botnet erkannt, wird es an den ESET Botnet-Tracker gesendet, der die genaue Malware-Variante bestimmt. Zudem werden mithilfe spezieller Entpacker und Entschlüsselungstools Informationen über den C&C Server und verwendete Kodierungs- bzw. Kommunikationsschlüssel extrahiert. Nach deren Erhalt wird von verschiedenen Standorten aus eine nachgebildete Kommunikation gestartet. Die extrahierten Daten werden anschließend zum Schutz aller ESET Kunden weiterverarbeitet, z.B. um URLs zu blockieren, neue Erkennungen für die Payloads zu erstellen oder die ESET Threat Intelligence Clients zu informieren.

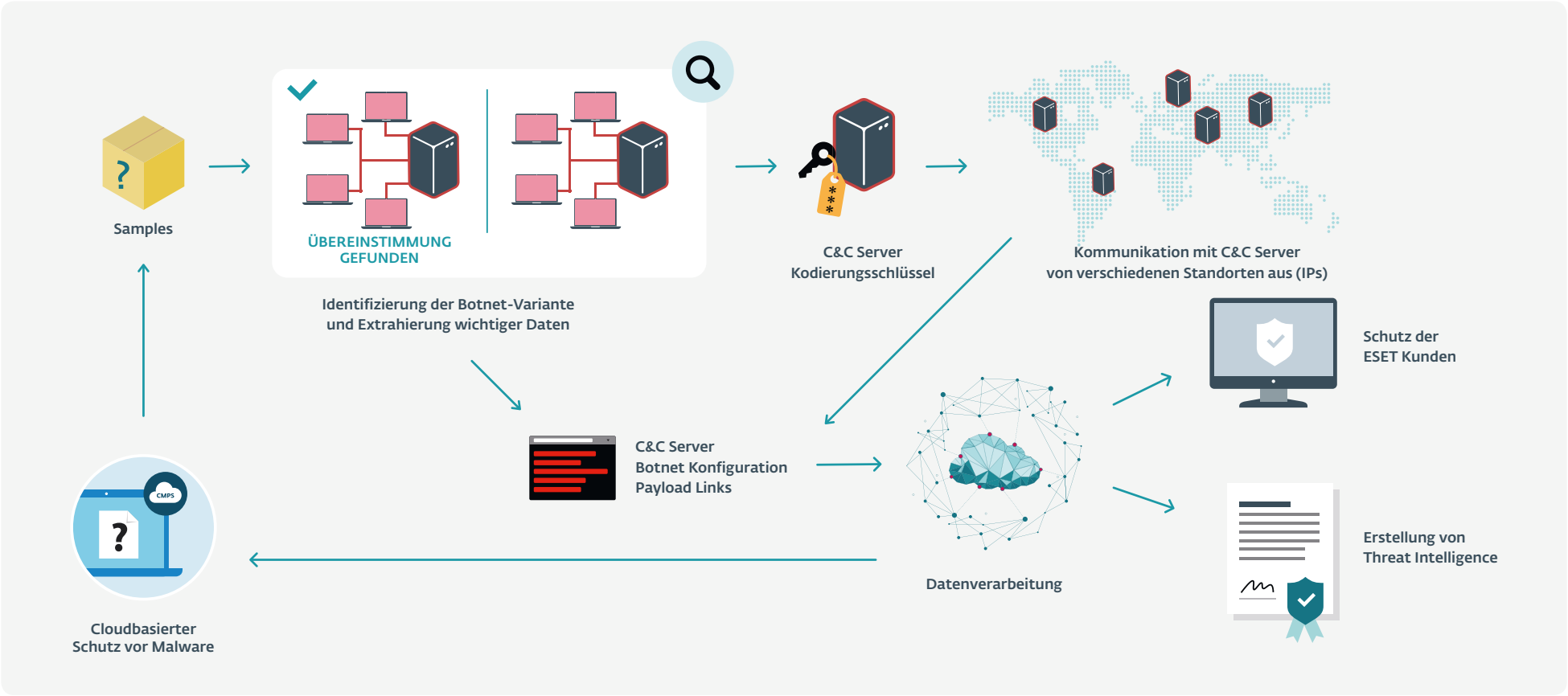


Abb. 9: Funktionsweise des ESET Botnet-Trackers

Threat Intelligence

ESET Threat Intelligence (ETI) unterstützt Unternehmen bei der Bekämpfung von zielgerichteten und verdeckten Cyberbedrohungen. Dank der Bereitstellung von Informationen aus mehr als 100 Millionen Sensoren erhalten Organisationen einen besseren Überblick über die aktuelle Bedrohungslage und können Angriffe vorhersehen und bereits im Vorfeld abwehren. Sollte es doch einmal zu einem Zwischenfall kommen, ermöglichen die Daten zudem eine schnelle und effektive Vorfallanalyse. Die umfangreichen Informationen schützen nicht nur das Business selbst, sondern auch die Endnutzer. Je nach Bedarf können ESETs Systeme und Experten individuelle Berichte über Botnets und zielgerichtete Malware anhand von YARA-Regeln, Phishing-Reports und Echtzeit-Datenfeeds im STIX/TAXII Format bereitstellen, die sich problemlos in bestehende SIEM-Tools implementieren lassen.

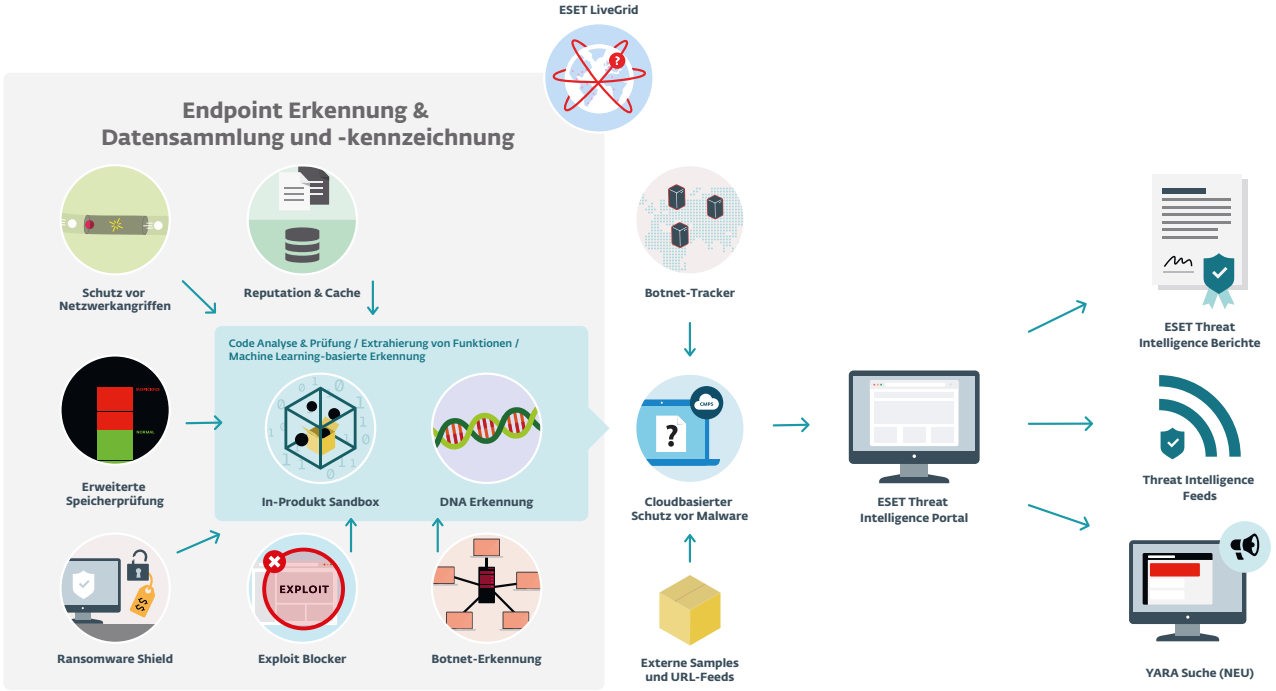


Abb. 10: Sammlung von Threat Intelligence durch ESET Technologien

REAKTIVER VS. PROAKTIVER SCHUTZ

DNA Erkennungen sind zwar wichtig für die Erkennung ganzer Malware-Familien, allerdings müssen sie dem Nutzer erst zur Verfügung stehen, um ihn zu schützen. Das gleiche gilt für die Scan Engine, Heuristik oder andere Anpassungen zum Schutz vor neuen Bedrohungen. Für das höchste Maß an Sicherheit ist die Kommunikation mit dem ESET LiveGrid Cloudsystem aus vielen Gründen wichtig:

- Offline-Prüfungen sind meistens reaktiv. Proaktiver Schutz bedeutet heute nicht mehr, dass ein Produkt über die beste Heuristik verfügt. Sobald ein Angreifer Zugriff auf die Sicherheits-Tools hat, macht es keinen Unterschied, ob man Signaturen, Heuristiken oder Machine Learning Klassifizierungen einsetzt: Ein Malware-Autor kann mit der Erkennungstechnologie experimentieren, die Malware solange modifizieren, bis sie nicht mehr erkannt wird und sie schließlich in freier Wildbahn einsetzen. ESET LiveGrid wirkt dieser Strategie entgegen.

- Updates bieten keinen Echtzeit-Schutz. Zwar können die Zeitintervalle zwischen den Updates so gering wie möglich gehalten werden, aber selbst dann geht es noch besser: Dank ESET LiveGrid werden Informationen bereitgestellt, sobald sie benötigt werden.

- Malware will meistens unentdeckt bleiben. Insbesondere bei Cyberspionage versucht ein Schädling, so lange wie möglich einer Erkennung zu entgehen. Bei zielgerichteten Angriffen wird Malware vereinzelt und nur an ausgewählte Ziele verbreitet. Diese Tatsache nutzen wir aus: Objekte, die nicht weit verbreitet sind und keine gute Reputation haben, werden als potenziell schädlich eingestuft und entweder auf dem Endpoint analysiert oder zur detaillierten automatischen Prüfung über unser LiveGrid Feedback-System eingereicht. Das ESET LiveGrid Reputationssystem beinhaltet Informationen über Dateien, deren Ursprung, Ähnlichkeiten, Zertifikate, URLs und IPs.cates, URLs and IPs.

Automatische und manuelle Verarbeitung von Samples

Jeden Tag erhält ESET Tausende an Samples, die nach Vorverarbeitung und Bündelung automatisch, halbautomatisch und manuell analysiert werden. Die automatische Analyse wird von intern entwickelten Tools auf mehreren virtuellen und physischen Maschinen durchgeführt.

Mithilfe verschiedener Attribute, die während der Ausführung entsprechend statischer und dynamischer Code-Analyse extrahiert werden, wie Änderungen am Betriebssystem, Muster in der Netzwerkkommunikation, Ähnlichkeiten zu anderen Malware-Samples, DNA Merkmale, strukturelle Informationen und Erkennung von Abweichungen, eine Klassifizierung vorgenommen.

Allerdings haben alle automatisierten Klassifizierungen Nachteile:

- Die Auswahl von Ausschlusskriterien für die Klassifizierung ist nicht gerade trivial und muss mithilfe von Expertenwissen getroffen werden.
- Die Klassifizierung über Machine Learning erfordert immer auch die Beteiligung von Menschen, um den für die Lernprozesse genutzten Input zu prüfen. Eine vollautomatisierte Analyse, bei der die vom System klassifizierten Samples als Input für das System genutzt werden, würde durch den Schneeballeffekt einer positiven Rückkopplungsschleife instabil werden. Nach dem Motto: „Abfall rein – Abfall raus."
- Die Machine Learning Algorithmen verstehen die Daten nicht und selbst statistisch korrekte Informationen sind nicht zwangsläufig verlässlich. So können selbstlernende Verfahren beispielsweise neue Varianten einer legitimen Software nicht von schädlichen Versionen oder an saubere Anwendungen gekoppelte Updater von einem von einer Malware genutzten Downloader unterscheiden. Zudem erkennen sie nicht, wenn legitime Software-Komponenten für schädliche Zwecke missbraucht werden.

- Beim Machine Learning führt das Hinzufügen von neuen Samples zum Lernprozess unter Umständen zu Fehlalarmen, deren Entfernung wiederum die Effektivität der Erkennung reduzieren könnte.
- Während die automatisierte Analyse eine unmittelbare Reaktion auf neue Bedrohungen über die Erkennung durch ESET LiveGrid ermöglicht, ist eine zusätzliche Verarbeitung von Samples durch Experten notwendig, um ein Maximum an Qualität sowie Erkennungsraten und gleichzeitig ein Minimum an Fehlalarmen zu gewährleisten.

Reputations-Dienste

ESET LiveGrid stellt zudem Reputationen für Objekte zur Verfügung. Wir bewerten die Reputation von verschiedenen Instanzen, einschließlich Dateien, Zertifikaten, URLs und IPs. Wie bereits beschrieben werden Reputationen genutzt, um neue schädliche Objekte oder Infektionsquellen zu identifizieren. Allerdings gibt es auch andere Einsatzbereiche.

Whitelisting

Durch Whitelisting wird die Anzahl an Prüfungen von Objekten durch die Scan Engine erheblich reduziert. Wurde ein Objekt bereits als sauber erkannt und nicht geändert, ist ein Scan nicht notwendig. Das sorgt für eine schnelle Performance und macht die ESET Produkte so robust – im Sinne von: „Der schnellste Code ist derjenige, der gar nicht ausgeführt wird." Unsere Whitelists werden kontinuierlich an die sich ändernden Gegebenheiten der Software-Welt angepasst.

Sammlung wertvoller Informationen

Die von Nutzern akzeptierte Bereitstellung von Informationen an ESET LiveGrid verwenden wir zur Beobachtung und Bekämpfung globaler Bedrohungen. Sie liefern uns wertvolles Datenmaterial, durch das wir besonders dringende Fälle identifizieren, aktuelle Malware-Trends beobachten und die Entwicklung neuer Sicherheitstechnologien planen können.

ÜBER IOCS

Sogenannte Indicators of Compromise (IOCs) werden innerhalb der heutigen Unternehmenssicherheit als sehr wichtig empfunden. Allerdings sind sie noch lange nicht so weit entwickelt, wie es manch ein Sicherheitsanbieter der „nächsten Generation" behauptet. Die folgende Grafik zeigt eine Aufgliederung der häufigsten IOCs sowie deren Grundlage.* Die Eigenschaften, auf die sie sich beziehen, sind offensichtlich relativ grundlegend: Bei einem Viertel der Fälle handelt es sich um MD5-Hashes, gefolgt von Dateinamen. Das verdeutlicht, dass diese Methode für die Abwehr nicht geeignet ist. Hilfreich ist sie hingegen bei der Forensik. Ironischerweise sind einige der Hersteller der „nächsten Generation", die eine signaturbasierte Erkennung ablehnen, begeistert von IOCs, obwohl sie tatsächlich die schwächste Art einer solchen Erkennung darstellen.

*Datenquelle: IOC Bucket, April 2015. IOC Bucket ist eine freie, von der Community betriebene Plattform, über die Informationen über Bedrohungen bereitgestellt werden.

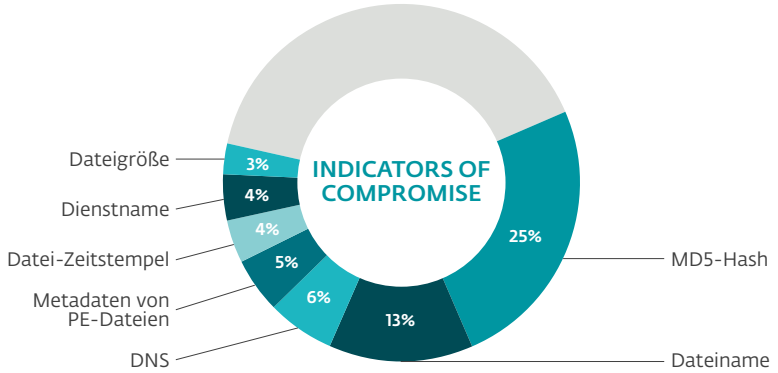


Abb. 11: Analyse der Indicators of Compromise von IOC Bucket (Sample von April 2015)

FAZIT

Es gibt kein Allheilmittel für IT-Sicherheit. Moderne Malware ist dynamisch und geht oftmals zielgerichtet vor. Deshalb bedarf es eines mehrschichtigen Schutzes, der auf proaktiven und intelligenten Technologien basiert, in deren Entwicklung die von erfahrenen Researchern über viele Jahre gesammelten Informationen eingehen. Schon vor 20 Jahren hat ESET die Zeichen der Zeit erkannt und den traditionellen AV-Ansatz erweitert, um auf die zunehmende Komplexität heutiger Malware zu reagieren. Deshalb haben wir unsere Scan Engine mit proaktiven Technologien und vielschichtigen Schutzmechanismen ausgestattet.

ESET ist einer der wenigen Sicherheitsanbieter, die aufgrund jahrelanger Erfahrung ein hohes Maß an Sicherheit gewährleisten können. Wir arbeiten unermüdlich daran, unsere Technologien weiterzuentwickeln, um den bestmöglichen Schutz zu bieten und den Malware-Autoren stets einen Schritt voraus zu sein. Mit der einzigartigen Kombination aus Endpoint- und cloudbasierten Technologien gehören unsere Produkte zu den zuverlässigsten Sicherheitslösungen auf dem Markt.


ENJOY SAFER TECHNOLOGY™