Prävention statt Erkennen & Reagieren

"Wir behaupten, dass echte Prävention die Kosten für Sicherheit senkt, die Komplexität abbaut und der beste Schutz gegen Malware ist."

Einführung

Die Risiken der Analyse bei Ausführung von Malware

Im Internet gibt es nur Opfer und potenzielle Opfer. Jeder ist gefährdet, von Einzelpersonen bis hin zu großen Unternehmen. Jede Minute werden der Angriffsfläche weitere Geräte hinzugefügt. Im Wettbewerb um die Verbesserung und Vertiefung der Verteidigung sehen sich Sicherheitsteams durch zunehmende Komplexität mit einer ständig wachsenden Herausforderung konfrontiert. Mehr Produkte, die mehr Ereignisse anzeigen und viele unterschiedliche Vektoren überwachen, machen es immer schwieriger, relevante und tatsächliche Indikatoren für Gefährdungen zu finden, wodurch sich die Sicherheitssituation verkompliziert, ohne dass die Sicherheit effektiv gesteigert wird. Diese steigende Komplexität verringert die Sensibilität und Reaktionsfähigkeit des Sicherheitsteams, wodurch die tatsächlichen Kosten der Betriebssicherheit in die Höhe getrieben werden.

Diese Situation haben die Verteidiger jedoch nicht selbst verursacht. Die Verbreitung von Anbietern und Produkten, angetrieben durch eine überwältigende Nachfrage und eine wachsende Sicherheitsbranche, hat eine breite Vielfalt von Ansätzen zur Lösung verschiedener Sicherheitsprobleme geschaffen. Bei der Suche nach einem neuartigen, oft informationszentrierten Blickwinkel, haben jedoch viele dieser Lösungen versehentlich neue Herausforderungen geschaffen und sind daran gescheitert, die Sicherheit zu verbessern.

Eine bestimmte Art von Malware ist teilweise an fast jedem sicherheitsrelevanten Ereignis beteiligt (berücksichtigt man, dass Insider an 10,6% der Vorfälle beteiligt sind[1]). Somit ist eine effektive Endpunkt-Sicherheitsstrategie eine der größten Herausforderungen für Sicherheits-Teams. In dieser Ausarbeitung untersuchen wir die aktuellen Strategien zur Angriffserkennung, die zunehmend an Popularität gewinnen. Wir werden die Gefahren einzelner Strategien erörtern, die sich nur auf die Analyse nach der Ausführung von Schadcode konzentrieren, und die zugrunde liegende Problematik bei der Erkennung von Malware besprechen, die ein Problem für die meisten Unternehmen darstellt.

Eine Evolution der Strategie

Strategien zur Angriffserkennung lassen sich in drei große Kategorien unterteilen, abhängig davon, wann sie eingreifen sollen: Bevor die Malware ausgeführt wird (vor der Ausführung), während der Ausführung (Ausführung) oder nach der Ausführung (post-Ausführung).

Vor der Ausführung	Ausführung	Nach der Ausführung
▪ Hash-basiert - (halb) automatisiert	▪ Speicher-basiert (Signatur)	▪ IDS
▪ Generisch und heuristisch (manuelle Signatur)	▪ IDS	▪ Speicheranalyse
▪ Basiert auf File-Reputation - Cloud lokal (Ende der 2000er Jahre)	▪ Exploit Erkennung	▪ Verhalten
▪ Policy (Whitelisting) (Ende der 2000er Jahre)		▪ SIEM (Analytik)
▪ Modelle, die auf maschinellem Lernen basieren (2012)		▪ "erkennen und reagieren" (ETDR)

Technologien zur Früherkennung von Malware verwenden generische und heuristische Signaturen, um eine Malware-Datei zu erkennen, sobald sie auf die Festplatte geschrieben wird. In der Vergangenheit waren Anbieter von Antivirus-Software (AV) in der Lage, Signaturen manuell zu schreiben, weil Malware-Familien sich nicht so oft verändert haben.

Für eine kurze Zeit, Kurzzeitig waren die Kosten für die Verwaltung von AV-Sicherheitslösungen im Unternehmen weitgehend festgelegt. Einmal installiert, lief eine AV-Lösung „auf Autopilot“ und erkannte und beseitigte Malware. AV-Lösungen mit ihren Heuristiken und Emulator-basierten Signaturen hatten die Oberhand bei diesem Kampf. Nicht so heute.

Mitte der 2000er Jahre kam eine Welle vielschichtiger, sich schnell verändernder Malware und Rootkits, die mit vielen Tricks ausgestattet waren, um den traditionellen Schutz von AV und den Laufzeitschutz zu umgehen. Um die Erkennungsraten hoch zu halten, entwickelten Anbieter von Sicherheitssoftware automatisierte Malware-Verarbeitungslösungen, die mit Hashing-Technologien ausgestattet waren. Der fatale Nachteil von Hashing besteht darin, dass alle Malware-Proben, egal wie gering die Unterschiede sind, anhand eines Hashes völlig neu und anders aussehen.

Die nächste Welle vielschichtiger Malware nutzte genau diesen Schwachpunkt der automatisierten Hashing-Technologien aus. Die Kosten durch nicht erkannte Malware sind für Unternehmen rapide angestiegen. Daher haben die Anbieter von Lösungen begonnen, Dienstleistungen für die Reparatur und Wiederherstellung in ihr Portfolio aufzunehmen. Um den Herausforderungen bei der Erkennung von bösartiger Software zu begegnen, hat die Industrie Speicheranalysen und Verhaltenstechnologien hinzugefügt. Weitere Sicherheitsschichten sind im Laufe der Zeit hinzugekommen.

Diese neueren Strategien zur Erkennung von Malware wurden geschaffen, um für das Versagen der AV-Lösungen, die Angriffe zu verhindern, zu kompensieren. Aus der Perspektive der kollektiven Sicherheitsindustrie lenkte dies den Fokus weg von der Investition in präventive Lösungen und andere Technologien, die die Kosten für das Sicherheitsmanagement in der Vergangenheit niedrig gehalten hatten.

Zu dieser Zeit wurden die reinen Policy-basierten Lösungen eingeführt, bei denen nur bekannte Dateien ausgeführt werden konnten (Whitelisting). Dieser Ansatz wurde streng auf bestimmte Anwendungsfälle beschränkt, die sehr restriktive Änderungskontrollen hatten, wie Point of Sale-Systeme, Geldautomaten und ICS/SCADA-Umgebungen.

Heute reagieren viele „hochmoderne“ Sicherheitslösungen auf die Zunahme der Cyber-Attacken durch Malware-Analysen nach der Ausführung (post-Execution). Dazu gehört die Überwachung von Endpunkten und die schnelle Reaktion auf Angriffe. Obwohl es wie das Gebot der Stunde zu sein scheint, müssen wir die Auswirkungen von diesem neuen Vorstoß verstehen und untersuchen, wie wir die Sicherheit am maximal verbessern.

Auf das Schlimmste gefasst?

Die Ausführung von Malware am Endpunkt birgt inhärente Risiken. Malware erreicht die post-Execution-Phase nach dem Scheitern aller präventiven Lösungen. Die Hoffnung der Anbieter von Post-Execution Malware-Analyse-Lösungen ist es, dass nun eine Aktion des Schadcodes das bösartige Verhalten enttarnt und dass das betroffene Unternehmen in der Lage ist, eine neue Überwachungsschicht zu nutzen, um eine Wiederherstellung zu ermöglichen. Die Überwachung nach der Ausführung protokolliert und analysiert das Verhalten von Anwendungen und in vielen Fällen auch einen Großteil des Netzwerkverkehrs. Dies soll dazu beitragen, Malware zu erkennen und im Falle eines unvermeidlichen Worst-Case-Szenarios eine Wiederherstelllung zu ermöglichen.

Das Schlüsselwort hier ist „Worst.“ Wir glauben, dass die IT-Sicherheitsindustrie mehr kann, als nur im schlimmsten Fall tätig zu werden.

Zurückkommend auf das Dilemma der Ausführung und Analyse von Malware auf dem Endpunkt, müssen wir die folgende Frage beantworten: Was sollen diese Lösungen überwachen? Diese Frage ist wichtig! Wenn eine Lösung die ist, dass in Erwartung des schlimmsten Szenarios die meisten Daten zu Netzwerk, Betriebssystem und Anwendungsverhalten erfasst wird, dann sammelt sie riesige Datenmengen

Lösungen, die erst nach der Ausführung aktiv werden, sind unvorteilhaft. Mit begrenzter Autonomie können sie einfach nicht riskieren, etwas Wichtiges zu verpassen, und sie versuchen daher, eine Lawine eine Lawine von Daten zu analysieren. Dazu gehört das Schreiben auf Datenträger (und Mutterprozesse), Ausführungsereignisse, RPC-Kommunikation, Benutzeraktivitäten (einschließlich Cookies usw., geschriebenen Cookies usw.), DNS-Anfragen und Netzwerk-Datenüberwachungs-Mitschnitte, wie PCAP oder NetFlow, bei allen Aktivitäten.

Diese Datenmenge summiert sich schnell. Gehen wir davon aus, dass ein solches System 1 Megabyte pro Stunde pro Host sammelt (entsprechend 1000 1-Kilobyte-Datensätze nach der Kompression). Multipliziert mit 24 Stunden für 1000 Hosts ergibt dies 24 Millionen Ereignissen oder 24 Gigabyte Daten pro Tag. Nach 90 Tagen häufen Sie 2,1 Milliarden Datensätze oder 2,1 Terabyte an Daten an. Man stelle sich vor, wie viele Daten ein Unternehmen mit 50.000 bis 100.000 Hosts sammeln würde.

Auch mit diesem unhandlichen Ansatz zur Datenerhebung sind Verteidiger vielleicht nie in der Lage, die Nadel im Heuhaufen zu finden. Dieser Ansatz ist äußerst komplex und verschwendet Energie, Arbeitsspeicher, Speicherplatz und Netzwerkressourcen. Betrachten wir einmal die versteckten Kosten eines Unternehmens, wenn eine Sicherheitslösung den Ansatz „Detect & Respond“ nur dann verwendet, nachdem die Malware ausgeführt wurde.

Verwaltungskosten

Das Sammeln und Pflegen der erforderlichen Informationsmengen, die für die Ausführung einer Lösung mit dem Ansatz „Detect & Respond“ benötigt werden, ist eine Anforderung, die mit der Zeit wächst, ebenso wie auch die Kosten für das Extrahieren von Kennwerten aus diesem Informationsberg ansteigen. Unternehmen sollten sich über die folgenden versteckten Kosten und Bedenken im Klaren sein:

Security-Event-Analyse

Zusätzliche sicherheitsrelevante Ereignis-Einträge erfordern weitere Analysen und erhöhen Kosten.

Endpunkt-Systemleistung

Kontinuierliche Endpunktüberwachung führt zu Performance-Engpässen, eine unnötige Datenerfassung belastet den Endpunkt.

Cloud-Lookups / Netzwerk-Bandbreite

Obwohl der Anbieter der Sicherheitslösungen für Cloud-Speicher bezahlt, ist es das Unternehmen, das die Datennutzung im eignen Netzwerk und die Auslastung der Netzwerkinfrastruktur trägt.

Vor-Ort-Analyse

Das Hosting und die Verwaltung einer großen Datenlösung (Big Data) vor Ort, um die massiven Datenvolumen zu bewältigen, erhöht die festen und variablen Kosten.

Bedenken hinsichtlich der Privatsphäre

Lösungen, die einen Großteil der Systemereignisse für die Erkennung und Response aufnehmen und speichern, sammeln am Ende mehr Informationen als notwendig oder erwünscht ist. Zugangskontrollen, Ort der Datenspeicherung, Aufbewahrungsfristen und Verschlüsselungsrichtlinien der gesammelten Daten können je nach Anbieter variieren.

Einige Sicherheitslösungen basieren auf öffentlich zugängliche Analysesysteme und Datenquellen, um Informationen über verdächtige Dateien zu erhalten. Diese Quellen liefern häufig keine nützlichen Daten, da Ansätze, die auf der Erkennung von Malware vor der Ausführung basieren, gravierend an Popularität verloren haben und Anbieter von Sicherheitslösungen nicht ausreichend investieren, um die Fähigkeiten bei der Dateierkennung zu verbessern.

So wurde die Malware Dyre beispielsweise im Juni an zwei aufeinanderfolgenden Tagen erkannt. Eine Abfrage, die ein beliebiger Anbieter am 4. Juni erhalten hat, hat die Probe, basierend auf dem kollektiven Wissen der Industrie, nicht als Malware erkannt, sondern erst einen Tag später. Es gibt viele Beispiele von Malware, die zunächst nicht als bösartig identifiziert wird und über Wochen, Monate oder Jahre zunächst nicht gemeldet wird. Diese Verzögerungen verdeutlichen den Bedarf an Systemen, um die Lücke bei der Identifizierung von Malware zu schließen, ohne sich dabei auf reaktive Datei-Scanner zu verlassen.

Was Sie sehen ist was, Sie kriegen

Erlaubt man die Ausführung von Malware, entstehen große technische Herausforderungen, da die Spielplätze für die Malware vergrößert werden, anstatt die Optionen zu limitieren. Dies sind einige Beispiele von Schwächen der „Detect and Respond“-Technologie.

Gutes Verhalten / schlechtes Verhalten

Während der Analyse von Malware während der Durchführung müssen Endpunkt-Lösungen den Verdächtigen in seiner natürlichen Umgebung überwachen, um Ereignisse zu erkennen, zu melden und zu blockieren und den Angriff zu stoppen und Daten wiederherzustellen. Bei einer solchen Überwachung ist es sehr schwer vorherzusagen, wann eine Malware, wie „Rombertik“ ihre hässliche Seite zeigt.[2,3,4] Es der kann Tage dauern, bis der schädliche Teil des Code ausführt wird. Weiterhin kann die Auslösung der Malware auch von Benutzeraktion abhängig sein (wie etwa in das Scrollen auf die zweite Seite in einem Dokument). Lösungsansätze zu diesen Problemen bleiben nicht lange erfolgreich und werden von Angreifern schnell umgangen.[5,6] Alternativ wäre es möglich, in Erwartung eines Sicherheitsvorfalles alle Anwendungen ununterbrochen zu überwachen, was wieder die Kostenfrage im Sicherheitsmanagement aufwirft.

Wie spät ist zu spät?

Kann eine Monitoring-Technologie das erste „schlechte Ereignis“ selbständig erkennen? Ist die Installation eines Treibers selbst ein böswilliges Ereignis? Meistens ist die Antwort nein, aber in dem Moment, in dem ein bösartiger Kernel-Treiber läuft, ist es wahrscheinlich zu spät, um das System zu retten. Dies sind nur einige der Nachteile der Überwachung nach der Ausführung von Code. Häufig stellt eine Reihe von Verhaltensweisen ein schädliches Verhalten dar. Wenn die richtige Bestimmung eines Verhaltens nicht rechtzeitig erfolgt und bedrohliche Ereignisse vor allem nicht jedes mal erkannt werden, kann es zu spät sein, um die schädigende Auswirkung von Malware zu blockieren. Es ist das alte Katz-und-Maus-Spiel bei der „Signaturerkennung“: Die Verteidiger versuchen, die Malware so früh wie möglich zu erkennen und die Angreifer versuchen dies zu umgehen, indem sie gutes und schlechtes Verhalten vermischen und damit die Aufdeckung erfolgreich stören.

Zu den Beispielen für irreversible Schäden der Verursachung von Malware, bei der eine Blockierung nicht in jedem Fall und nicht rechtzeitig erfolgt, zählen:

Parasitäre Infektion

Durch die Ausführung parasitärer Malware steigen die Kosten zur Rettung und Wiederherstellung von Systemen und Dateien drastisch an. Eine Datei kann irreparabel beschädigt sein, und es kann notwendig sein das System neu aufzubauen oder aus dem (hoffentlich nicht befallenen) Backup wiederherzustellen.

Datenvernichtung

Wir haben vor kurzem zwei große Angriffe gesehen, die nicht durch den alleinigen Detect-and-Respond-Ansatz hätten verhindert werden können. Bei den Angriffen auf Saudi Aramco und Sony Pictures wurde jeweils ein signierter, kommerzieller Kernel-Treiber verwendet, um die Zielmaschinen zu löschen und Daten zu zerstören.[7]

Ein weiteres einfaches Beispiel ist die Ausführung von Ransomware wie CryptoWall/CryptoLocker, die jede Datei im System verschlüsselt und dann Erpressungsgelder verlangt. Lösungen, die nach der Ausführung aktiv werden, erkennen diese Angriffe zu spät, oder auch gar nicht. Die betroffenen Systeme können später nicht wiederhergestellt werden. Dies wird im Video „CylancePROTECT® gegen Ransomware“ demonstriert.[8]

Malware erkennt Sicherheitssoftware und Analyseumgebungen

Jüngste Untersuchungen an der „Rombertik“ Malware zeigt ein gutes Beispiel für die Verwüstung auf, die verursacht werden kann, wenn Malware zur Ausführung kommt. „Rombertik“ versucht, Sicherheitskontrollen gezielt zu umgehen und Umgebungen und Maschinen zu zerstören, die versuchen die Malware zu analysieren.[9]

Daten-Exfiltration

Im Laufe der Jahre haben wir viele Arten von Point of Sale-Malware gesehen, wie beispielsweise Framework POS, die einen DNS-Mechanismus verwendet hat, um Kreditkartendaten zu exfiltrieren, oder die berüchtigte BlackPOS Malware, die ihre Opfer 2013 gefunden hat. Die Erkennung nach der Ausführung hätte das Infektionsrisiko mit dieser speziellen Malware nicht reduziert. Haben die Daten das System erst einmal verlassen, ist es praktisch unmöglich, den Schaden wieder rückgängig zu machen. Sobald der schädliche Programmcode ausgeführt wird, hat er viele Möglichkeiten um Daten, zu versenden. Damit sind erneut die Anbieter von Sicherheitslösung gefragt, die nun aus dem gelernten Schaden wieder eine Vilezahl von Abwehrmechanismen entwickeln müssen.

Angriffe auf Sicherheitslösungen

Das Zulassen der Ausführung von Malware hat einigen schädlichen Programmen die Möglichkeit gegeben, Sicherheitslösungen und Endpunkt-Pakete direkt anzugreifen. Zum Beispiel versuchte die Malware „Vawtrak“ letztes Jahr gezielt Sicherheitssoftware mit Policies für die Einschränkung von Software zu deaktivieren.

Zurück in die Zukunft

Was haben Anbieter und Anwender von Sicherheitssoftware aus fast einem Jahrzehnt der erhöhten Sicherheitskosten und gestiegenen Anforderungen an IT-Sicherheitslösungen gelernt? Wenn es eine Sache gäbe, die wir hätten anders machen könnten, was wäre das?

Es ist klar, dass es nicht reicht auf Lösungen zu vertrauen, die Malware nur NACH der Ausführung erkennt. Als die Sicherheitsindustrie begann, sich von der Eindämmung vor der Ausführung abzuwenden, wurden Technologien reaktiv im hohen Maße abhängig von manueller Analyse und Signaturerstellung. Sicherheitsanbieter hofften, dass Analysen und Lösungsansätze nach der Ausführung ihnen effektiver beim Kampf gegen das Malware-Problem helfen. Die Realität zeigt aber, dass die gesamte Sicherheitsarchitektur dadurch komplexer, teurer und trotzdem anfälliger für Angriffe geworden sind.

Cylance® hat diese Herausforderungen durch die Entwicklung der ersten und einzigen Schutztechnologie für die Erkennung und Verhinderung von Malware vor der Ausführung gemeistert, die auf künstlicher Intelligenz und maschinellem Lernen basiert. Die größte Herausforderung besteht darin, das Programm zu analysieren und nur basierend auf den Informationen aus der Datei selbst zu bestimmen, ob eine Datei gut oder schlecht ist - und das ganze in einem massiven Umfang. Die Möglichkeit, dies mit einer großen Anzahl von Samples durchzuführen ist wichtig, weil die heutige Entwicklung von Malware in hohem Maße automatisiert ist. Heute ist der Aufwand von Angreifern für die Mutation von Malware verschwindend gering. Manuelle, allgemeine Signaturen (Emulations- oder Heuristik-basiert) waren ausreichend, als die Erstellung von Malware noch manuell erfolgte, ist es aber heute nicht mehr.

Um sich wieder auf die Grundlagen zu besinnen und Malware noch vor der Ausführung zu stoppen, nutzt Cylance maschinelles Lernen, um mathematische Modelle zu generieren, die vorhersagen können, ob ein Programm bösartig ist. Dieser Ansatz für die Dateianalyse hat sich als äußerst wirksam für die Erkennung von Malware erwiesen. Cylance hat bewiesen, dass es möglich ist, Malware mit erstaunlicher Genauigkeit zu identifizieren, ohne sie jemals zuvor gesehen zu haben. Kommen wir nun nochmal zurück auf unser Dyre Beispiel: So ist es Cylance erfolgreich gelungen, die Malware mit einem maschinellen Lernmodell zu erkennen, das bereits im August 2014 veröffentlicht wurde - 10 Monate vor der Veröffentlichung der Variante. Cylance ist es gelungen, Dyre vor der Ausführung zu erkennen und lange bevor es von traditionellen AV-Lösungen im Feld identifiziert wurde und erste Unternehmen befallen wurden.

Die Erkennung von Malware vor der Ausführung ist kein Allheilmittel, an dem keine Malware jemals vorbeikommt. Keine einzige Lösung kann unfehlbar sein. Wie Anwender von Sicherheitslösungen wissen, geht es bei der Sicherheit um die Minimierung von Risiken und die möglichst nahe Annäherung an absolute Sicherheit.

Eine Strategie, die auf die Erkennung von Malware bereits vor der Ausführung abzielt, ist der erste Schritt, um ein effektives Sicherheitsportfolio aufzubauen. Die Identifizierung von bösartigen Anwendungen, bevor diese überhaupt eine Chance auf Ausführung erhalten, hilft, die Kosten für Sicherheitsmanagement und, gleichzeitig die Auslastung von Systemen durch den Virenschutz zu senken. Damit sinkt die Anzahl der Angriffe die überhaupt zur Ausführung gelangen und damit eine Überwachung benötigen. Dies ermöglicht eine Reduzierung der Sicherheitsschichten, die erforderlich sind, um erfolgreiche Angriffe zu vereiteln.

Schlussfolgerung

Die IT-Sicherheitsindustrie hat bei der Verteidigung gegen böswillige Angriffe einen langen Weg zurückgelegt. Doch in der Eile, schnelle, einfache „out-of-the-Box“-Lösungen zu entwickeln, ist die Industrie in einem Teufelskreis der Signaturen stecken geblieben: Anbieter entwickeln neue

Über Cylance

Cylance ist das einzige Unternehmen, das eine präventive Lösung für die Cyber-Sicherheit anbietet, die hochentwickelte Bedrohungen und Malware an der empfindlichsten Stelle stoppt: dem Endpunkt. Durch einen revolutionären Ansatz mittels künstlicher Intelligenz analysiert CylancePROTECT, die Endpunkt-Sicherheitslösung von Cylance, die DNA des Codes vor der Ausführung auf dem Endpoint, um Bedrohungen zu finden und zu verhindern. Dazu nutzt das Produkt lediglich einen Bruchteil der Systemressourcen, die Anti-Virus- sowie Detection-Lösungen benötigen, die heute im Einsatz sind. Weitere Informationen finden Sie auf www.cylance.com

Lösungen, die Autoren von Malware finden Techniken um diese zu umgehen dann entwirft die Sicherheitsindustrie weitere Teillösungen, was zu wiederum neuen Umgehungstaktiken und Angriffen führt.

Viele Sicherheitslösungen versuchen nun, das Problem der Erkennung von Malware mit Ansätzen anzugehen, die den „Detect & Respond"-Ansatz verfolgen. Die Angreifer haben mit der Weiterentwicklung der Malware aber mehrere Möglichkeiten gefunden, diese Lösungen anzugreifen und zu umgehen.

Diese Ansätze sind nicht nur unwirksam, „Detect & Respond" - Lösungen generieren so viele Daten, dass schnell wachsende technische und personelle Anforderungen für die groß angelegte Analyse zur Datensicherheit entsteht, die die Industrie vermutlich überhaupt nicht verwalten kann.

Neue Sicherheitsschichten müssen genau darauf eingestellt sein, was wann zu überwachen ist. Wenn eine Lösung großzügig alle möglichen Daten erfasst, ist dies eher eine Vorbereitung auf eine eventuelle Wiederherstellung nach einem Vorfall, nicht aber der Versuch, den Vorfall im Vorfeld zu stoppen. Dies ist eine sehr riskante Haltung, denn wenn die Verteidiger jegliche Hoffnung aufgeben, die Angriffe jemals zu vereiteln, dann werden Sie immer zu spät sein und im besten Falle nur Schadensbegrenzung betreiben. Das ist keine akzeptable Lösung.

Referenzen

1 http://www.verizonenterprise.com/DBIR/2015/

2 http://blogs.cisco.com/security/talos/rombertik

3 http://joe4security.blogspot.com/2012/10/defeating-sleeping-malware.html

4 http://www.networkworld.com/article/2163341/byod/-sleeper--malware-like-nap-trojan-nothing-new.html

5 http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.361.9423

6 https://www.lastline.com/papers/acm_ccs11_hasten.pdf

7 http://arstechnica.com/security/2014/12/sony-pictures-malware-tied-to-seoul-shamoon-cyber-attacks/

8 https://www.youtube.com/watch?v=RkbB8pV09E8

9 http://blogs.cisco.com/security/talos/rombertik

+49-89-244455571
sales@cylance.com
www.cylance.com
Second Floor, 89/90 South Mall, Cork City, Ireland T12 RPP0

CYLANCE™