WannaCry Ransomware-Angriff
FAQ aus dem Webinar vom 16. Mai 2017

Q: Erkennt Trend Micro mittlerweile den Schädling?
A: Trend Micro hat sehr früh geschützt. Die proaktiven Schutzmechanismen wie Predictive Machine Learning und Behavior Monitoring haben seit Stunde Null geschützt. Die Regeln der Vulnerability Protection und Deep Security haben zudem den genutzten Exploit bereits seit März 2017 abgewehrt.

Q: Ist Windows 2000 ebenfalls durch WannaCry angreifbar?
A: Ja

Q: Wie sinnvoll ist es aus Ihrer Sicht, als Notmaßnahme das SMB1 Client/Server Protokoll einfach abzuschalten?
A: Sollten Sie nicht patchen können, halten wir diesen Schritt für sehr sinnvoll!

Q: Haben Sie eine Vermutung, wieso überhaupt ein Killswitch eingebaut war?
A: Es wird vermutet, dass der Killswitch als Teil einer Sandbox Evasion Taktik fungieren sollte.

Q: Was ist mit Perimeter gemeint?
A: Firewall/Gateways sind hier gemeint.

Q: Ist die Web Reputation kontraproduktiv? (falls die URL von Trend blockiert wird)?
A: Grundsätzlich nein. Weil die Killswitch Domain keine schlechte Reputation hat, wird sie auch nicht geblockt.

Q: Wie reagiert Hosted Email Security?
A: Bei schadhaften Emails kann das Attachment geprüft werden. Ebenso ist Webreputation in der Lage, Links zu bewerten. Die ankommende Email wird zudem in einer Sandbox geprüft. Der Schutz ist also umfassend für die initiale Email.

Q: Wann kommt die neue Worry-Free Version heraus und wird diese auch Predictive Machine Learning haben?
A: Worry-Free Services wurde vor kurzem in neuer Version mit Machine Learning herausgebracht. Die on-premise-Version wird wohl im Herbst inkl. Machine Learning kommen.

Q: Wie schaut es mit Worry-Free aus?
A: Worry-Free bietet als Lösung ebenfalls aktuelle Funktionen, um diese Bedrohung zu erkennen. Behavior Monitoring und Reputation bieten an dieser Stelle den Schutz an.

Q: Wie ist der Schutz bei den Worry-Free-Lösungen?
A: Der Schutz ist bei Worry-Free Produkten ebenfalls möglich. Behavior Monitoring unter anderem bietet hier die Möglichkeit zur Entdeckung und Schutz.

Q: Kann Deep Security zusätzlich zu Worry-Free installiert bzw. genutzt werden?
A: Wenn Sie die Deep Security Funktionen nutzen wollen, dann raten wir zu entweder Deep Security oder OfficeScan mit Vulnerability Protection. Der Worry-Free-Agent und der Deep Security Agent auf einem System ist nicht sinnvoll.

Q: Erkennt Hosted Email Security die embedded URL / Dropboxlink bzw. Word Attachment?
A: Bei den bekannten Fällen wurde das Attachment erkannt und abgewehrt.

Q: Hat Deep Discovery Email Inspector den Angriff ebenfalls erkannt?
A: Ja

Q: Was passiert, wenn ein infizierter Win10 PC mit einem SMB-Share eines 2008 SBS verbunden wäre?
A: Sofern der Server 2008 verwundbar ist, wird das Betriebssystem mit dem Krypto-Trojaner infiziert. Allerdings passiert dies nicht erst beim Verbinden des Shares, sondern bereits vorher, wenn der Server durch den infizierten Client mittels Netzwerkscan gefunden wurde.

Q: Muss man die Scan Engines auch updaten?
A: Nein. Ein Pattern-Update reicht. Wenn in Einzelfällen Engine-Updates angeboten werden, dann hat dies nichts mit der Angriffswelle zu tun. Installieren Sie dann dennoch bitte das Update, um auf dem neuesten Stand zu sein.

Q: Im Deutschlandfunk sagte ein Experte im Interview als Rat an Befallene Firmen - sofort bezahlen! Was halten Sie davon?
A: Absolut nichts. Die Empfehlung lautet: Nicht bezahlen. Damit würde man die Kriminellen nur unterstützen und finanzieren, und zudem ist man nicht sicher, ob die Daten tatsächlich entschlüsselt werden. Das Bundesamt für Sicherheit in der Informationstechnik rät im Übrigen ebenfalls, nicht zu zahlen.

Q: Wird der Microsoft Patch MS17-010 beim automatischen Windows Update automatisch installiert?
A: Ja

Q: Wie sieht es aus im Privatanwender Bereich mit Trend Micro Maximum Security?
A: Maximum Security schützt ebenfalls vor der Bedrohung. Bitte stellen Sie sicher, dass Sie die Microsoft Patches installiert haben sowie ein aktuelles Pattern File nutzen.

Q: Erkennt die Interscan Viruswall diesen Trojaner?
A: Die Viruswall kann anhand der Webreputation gefährliche Quellen sowie die C&C Kommunikation sehen und verhindern. Beim Email-Scan werden zudem schadhafte Attachments gesehen. Die InterScan Viruswall ist allerdings gegen die Verbreitung des Schädlings via MS17-010 machtlos.

Q: Sollte ich Worry-Free Advanced auch die Verhaltensüberwachung aktivieren?
A: Wir empfehlen dies. Schalten Sie Sicherheitsfunktionen nur dann ab, wenn Sie den Betrieb stören und es keine anderweitige Lösung gibt.

Q: Gibt es den Verschlüsselungsschutz auch in einer Worry-Free Variante?
A: Ja, Worry-Free hat Funktionalitäten zum Schutz vor Ransomware.

Q: Ein Experte meinte, Rechner nicht anzuschalten, wenn diese möglicherweise betroffen sind. Er riet dazu ein Backup zu machen mithilfe eines vom USB Stick gestarteten Systems, anstatt den direkten Start.
A: Grundsätzlich ein cleveres Vorgehen. In den meisten Fällen wird man wahrscheinlich nicht die Zeit haben, dies durchzuführen. Ansonsten verhindert das Booten eines Live-Systems die Verschlüsselung bzw. weitere Verschlüsselung. Allerdings sollten Backups natürlich bereits vor der Verschlüsselung existieren.

Q: Sind Linux Freigaben auch gefährdet?
A: Linux ist nicht betroffen; die Dateien auf dem Share hingegen könnten verschlüsselt werden.

Q: Behavior Monioring kann aber auf Servern nicht global aktiviert werden oder?
A: Seit dem OfficeScanXG SP1 ist das über eine Änderung der ofcscan.ini möglich. Sprechen Sie unseren Support oder Ihren Reseller/Distributor darauf an.

Q: Hilft RUBotted?
A: Nein

Q: Sind Windows-Phone-Handys infizierbar und/oder können sie als Quelle für die Erstinfektion von Windows-Versionen dienen?
A: Windows Phone ist nicht auf dem MS Bulletin 17-010 gelistet.

Q: Hat man den Stecker gezogen und fährt die Maschine dann wieder hoch, was passiert dann? Verschlüsselt der Schädling einfach weiter oder nicht?
A: Es wird weiterverschlüsselt. Sie sollten das System in einem solchen Fall vom Netz trennen und mit einem Live-System starten, wenn Sie noch auf das Dateisystem (oder Teile davon) zugreifen wollen.

Q: Wenn ein Solaris oder Linux die Freigabe zur Verfügung stellt, wird diese Freigabe (Netzlaufwerk, sofern gemappt) dann verschlüsselt?
A: Ja – wenn die Dateien durch einen Client im Zugriff sein können, und der Client die Dateien ändern/schreiben darf, werden auch diese verschlüsselt.

Q: Werden bereits verschlüsselte Systeme (BitLocker / VeryCrypt) nochmals verschlüsselt?
A: Ja. Die Dateien werden nochmals verschlüsselt.

Q: Was kann oder soll man tun, wenn man trotz aller Vorsichtsmaßnahmen und Patches etc. betroffen ist? (kann das überhaupt passieren?)
A: Es gibt leider keinen 100%igen Schutz. Wenn Sie dennoch betroffen sind, stellen Sie die Systeme wieder her und schreiben Sie die Daten zurück (Backup/Recovery).

Q: Reichen die administrativen Freigaben zur Weiterverbreitung/Infektion aus?
A: Ja. Ausschlaggebend ist nicht, welche Freigabe existiert. Der Exploit betrifft das SMB Protokoll, welches aktiv ist, sobald eine Freigabe angeboten wird.

Q: Wie kann man das eigene Netz auf die SMB-Schwachstelle scannen?
A: Schwachstellenscanner bieten die Funktion. Zum Beispiel „nmap“ oder „nessus“